دراسات عالمية

Panton 340 C



التلويح بقدرات الهجوم عبر الإنترنت

مارتن سي. ليبيكي

تصوير

أحمد ياسين



مركز الإمارات للدراسات والبحوث الاستراتيجية

العدد 124



تصوير
أحمد ياسين

التلويح بقدرات الهجوم عبر الإنترنت

مركز الإمارات للدراسات والبحوث الاستراتيجية

أنشئ مركز الإمارات للدراسات والبحوث الاستراتيجية في أبوظبي بتاريخ 14 آذار/ مارس 1994؛ كمؤسسة بحثية مستقلة تعنى بدراسة القضايا الاستراتيجية السياسية والاقتصادية والاجتماعية والمعلوماتية، التي تهم دولة الإمارات العربية المتحدة ومنطقة الخليج العربي خصوصاً والعالم العربي عموماً، ومتابعة أهم المستجدات الإقليمية والدولية.

وفي إطار التفاعل الثقافي والتعاون العلمي، يصدر المركز سلسلة **دراسات عالمية** التي تعنى بترجمة أهم الدراسات والبحوث التي تنشر في دوريات عالمية مرموقة، وتتصل موضوعاتها باهتمامات المركز العلمية، كما تهتم بنشر البحوث والدراسات بأقلام مشاهير الكتاب ورجال السياسة. ويرحب المركز بتلقي البحوث والدراسات المترجمة، وفق قواعد النشر الخاصة بالسلسلة.

رئيس التحرير: **راشد سعيد الشامسي**

دراســات عـالميــة

التلويح بقدرات الهجوم عبر الإنترنت

مارتن سي. ليبيكي

العـدد 124

تصوير
أحمد ياسين

تصدر عن



مركـز الإمـارات للدراسـات والبحـوث الاستـراتيجيـة

محتوى الدراسة لا يعبر بالضرورة عن وجهة نظر المركز

This is an authorized translation of the *Brandishing Cyberattack Capabilities*, by Martin C. Libicki, and published by the RAND Corporation (2013). The ECSSR is indebted to the author and original publisher for permitting the translation, publication and distribution of the above title under its name.

© مركز الإمارات للدراسات والبحوث الاستراتيجية 2014

حقوق الطبع والنشر محفوظة

الطبعة الأولى 2014

ISSN 1682-1211

النسخة العادية ISBN 978-9948-14-800-5

النسخة الإلكترونية ISBN 978-9948-14-801-2

توجه المراسلات باسم رئيس تحرير سلسلة **دراسات عالمية**

على العنوان الآتي:

مركز الإمارات للدراسات والبحوث الاستراتيجية

ص ب: 4567

أبوظبي، دولة الإمارات العربية المتحدة

هاتف: +9712-4044541

فاكس: +9712-4044542

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

المحتويات

ملخص 7

الفصل الأول: لا استعراضات في عيد العمال 17

الفصل الثاني: الآثار العامة للتلويح بقدرات الهجوم عبر الإنترنت 23

الفصل الثالث: التلويح بالهجوم عبر الإنترنت في مواجهة نووية 44

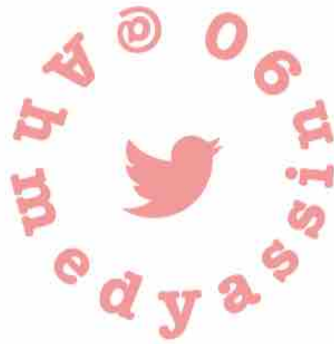
الفصل الرابع: الاستنتاجات 60

الهوامش 63

المراجع 71

نبذة عن المؤلف 75

تصوير
أحمد ياسين



تصوير
أحمد ياسين
تويتر
@Ahmedyassin90

ملخص

الخلفية والهدف

لا ينحصر الغرض من وجود القوات العسكرية الأمريكية في القتال وتحقيق النصر في الحروب فحسب، بل في الردع أيضاً؛ أي حثّ الآخرين وإقناعهم على عدم شنها (أو حتى التحضير لها). ولا يكون الردع ممكناً إلا إذا علم الآخرون ما تستطيع القوات العسكرية أن تفعله، أو على الأقل كانت لديهم دلالات جيدة عليه. ويكمن مثل هذا الإقرار أو الاعتراف في صلب استراتيجية الردع النووي الأمريكية، ويسهم - بدرجة أقل - في احتفاظ الولايات المتحدة الأمريكية بقوات تقليدية متنقلة قوية تستطيع التدخل في أي مكان تقريباً على وجه البسيطة.

إن قدرات الهجوم عبر الإنترنت تناقض مثل هذا الطرح؛ إذ لا أحد يعلم تماماً، أو حتى بصورة تقريبية، ما سيحدث إذا تعرضت دولة لهجوم شامل عبر الإنترنت، على الرغم من كثرة النشاط العدائي في الفضاء الإلكتروني. يتمثل أحد الأسباب في أنه لم تحدث حرب عبر الإنترنت، بمعنى حدوث هجمات يصحبها تدمير وخسائر في الأرواح مقارنة بالحرب المادية. كما أن النظرية تناقض ذلك الطرح؛ فالعيوب ونقاط الضعف في الأنظمة المستهدفة تجعل الهجمات عبر الإنترنت ممكنة. إنّ كشف العيوب التي تجعل الهجوم ممكناً هو بمنزلة إخبار الآخرين بشأن كيفية إصلاح هذه العيوب، ومن ثم، يقومون بالتخلص منها وتحييدها. وليس من المستغرب أن تُعتبر قدرات حرب الإنترنت الوطنية سراً يخضع لحراسة مشددة.

إن عدم إمكانية استخدام قدرات الهجوم عبر الإنترنت بسهولة لصوغ سلوك الآخرين لا يعني أنه لا يمكن استخدامها مطلقاً. وهذه الدراسة تستقصي الطرق التي يمكن من خلالها "التلويح" بقدرات الهجوم عبر الإنترنت، والظروف التي يمكن في ظلها

تحقيق بعض آثار الردع.[1] ثم تفحص العقبات التي تحول دون ذلك، وتعرض بعض القيود الواقعية على التوقعات.

من منظور السياسة العامة لم تقل الولايات المتحدة الأمريكية مطلقاً إنها ستستخدم الهجمات عبر الإنترنت، ولكنها لم تقل أيضاً إنها لن تستخدمها. كما أنها لم تجادل بقوة بشأن فكرة أن لها يداً في هجمات "ستكسنت" Stuxnet على المنشأة النووية الإيرانية.

الآثار العامة للتلويح بقدرات الفضاء الإلكتروني

يتعين على أي دولة تريد أن تثني دولاً أخرى عن العدوان في العالم المادي أو الفضاء الإلكتروني من خلال التلويح بقدرات الهجوم عبر الإنترنت، أن تسأل نفسها أولاً عما إذا كان الهدف من فعل ذلك هو الظهور بمظهر القوة أو جعل الآخرين يظهرون بمظهر العجز. وعلى الرغم من أن كلا الهدفين مفيد؛ فإن هناك حاجة إلى التركيز على رسالة واحدة في حملة اتصالات استراتيجية توحي بفائدة اتخاذ خيار. ثمة فائدة في التركيز على القوة الذاتية؛ وتتمثل في حث جميع الخصوم الفعليين والمحتملين على الحذر، وصرف المعتدين نحو فريسة أسهل. كما قد تعكس أيضاً بشكل جيد مصادر أخرى للقوة الوطنية. ولكن العزف على وتر نقاط ضعف الآخرين يسهم في ردع الدول المزعجة من خلال تذكيرها بنقاط ضعفها. كما أن ذلك يبعد الاتهامات بالترويج الذاتي من خلال تحويل التركيز باتجاه ضحايا محتملين.

ثمة تحدّ أكبر يتمثل في الكيفية التي يجري بها إظهار قدرات الهجوم عبر الإنترنت. إن أوضح طريقة لإظهار القدرة على اختراق نظام عدو ما، هي تنفيذ ذلك عملياً، وترك أثرٍ، على شكل بطاقة دعوة، مع تمني أن يتم إيصالها إلى صناع القرار الوطنيين. وإذا أمكن تكرار الهجوم بحرّية، أو إذا كان الاختراق مستمراً، فسيتم إجبار الجهة المستهدَفة على الإيمان بقدرة المهاجم على الولوج إلى نظامه في أي وقت من الأوقات. ويجب أن يُجبِر ذلك الجهة المستهدَفة على إعادة حساباتها بشأن علاقتها بالقوى المهاجمة.

لكن كما هي الحال في أمور كثيرة في الفضاء الإلكتروني، يبدو الأمر أبسط مما هو عليه. ومن الصعب التلميح إلى نجاح مباشر دون التسليم بمشاركة المرء في إلحاق الأذى في المقام الأول، ومن ثم بشرعية الحرب عبر الإنترنت كأداة من أدوات إدارة شؤون الدولة، وهو أمر لم تبادر الدول إلى الاعتراف به إلا في منتصف عام 2012. ومن شأن الأهداف القليلة القيمة أن تكون سهلة، إلا أن اختراقها ليس مثيراً للاهتمام. أما الأهداف التي تتمتع ببعض القيمة فهي - لذلك السبب - أصعب بكثير؛ ويعود ذلك غالباً إلى أنها معزولة إلكترونياً. وأخيراً، فإن القدرة على اختراق نظام ليست بالضرورة دليلاً على القدرة على تعطيل ذلك النظام وتدميره؛ فهذا لا يتطلب اختراق مستويات متميزة بدرجة كافية فحسب، بل معرفة كيفية جعل النظام يفشل في أداء المهمات ويبقى كذلك. ولكن قد يكون الاختراق في حد ذاته مروّعاً بما فيه الكفاية إذا لم تستطع القيادة المستهدفة تمييز الفرق بين الاختراق والتعطيل التام.

يُعتبر تعطيل نظام ما أكثر عدائية وأشد صعوبة من اختراقه؛ فهو يتطلب فهماً لما يجعل النظام يصاب بالفشل. وكذلك، فإن الحصول على النتائج المرجوة يتطلب أيضاً تحديد شكل الهجوم بحيث لا يستطيع الذين يديرون النظام كشف الهجوم وإصلاح الأضرار بسرعة؛ لأن إعلام الآخرين بالقدرة على تعطيل نظمهم وإبقائها كذلك ليس بالأمر السهل، وقد تتمكن الجهات المستهدَفة، من ثم، من خلال عمليات استعراض القدرات تلك من التعرف على نقاط الضعف التي سمحت بشن ذلك الهجوم، ثم إصلاحها. وإذا كان الأمر كذلك، ولكي ينجح التلويح بشن الهجوم، فقد تتطلب قدرات الهجوم عبر الإنترنت تكرار عمليات استعراض القدرات. وكبديل لذلك، يمكن أن يكون هناك استعراض للقدرة أقل عداء بحيث يجري التلاعب بالنظام وليس الإضرار به؛ فثمة خيط رفيع يفصل بين الأمرين.

هل بإمكان التلويح أن يساعد في ثني الدول الأخرى عن السعي لامتلاك قوة التقنية العالية والمتعلقة بالشبكات لمواجهة القدرات العسكرية الأمريكية؟ إن أفضل سبيل

للبرهنة على خطر الارتباط بالشبكات هو اختراق النظم العسكرية لإظهار هشاشتها (وبهذا الصدد، فإن ادعاء المسؤولية عن القيام بهذا الاختراق ليس ضرورياً، فالهدف ليس تأكيد قوة الولايات المتحدة، بل تأكيد ضعف نظم العدو القائمة على الشبكات وانكشافها). وفي ظروف أخرى، قد لا يكون إيضاح نقاط الضعف [لدى الخصم] ضرورياً، بل قد يكون فعلاً غير حكيم؛ فكل عملية اختراق تقود إلى مشكلات أو مآزق تجعل الاستغلال التالي أشد صعوبة. لكن التلويح بهجوم لا يترك أثراً محدداً، ومن ثمّ، فإنه لا يترك شيئاً محدداً لإصلاحه. والغرض هو إقناع الآخرين بأنهم لا يمكنهم حماية نظمهم حتى بعد بذل اهتمام وثيق بأمنها. وقد تكون نقاط ضعف الدول الأقل تطوراً وانكشافها أمام التلاعب والمناورة الخفية أكبر عندما تكون غير مدركة للتقنية التي ترتكز عليها نظم أسلحتها. وغالباً ما يؤدي فقدان الجهة المستهدَفة إمكانية الوصول إلى شيفرة مصدر الآخرين، وكذلك عدم بناء شيفرة خاصة بها، إلى تعقيد تصور المشكلة ومن ثم صعوبة معرفة كيف يمكن إصلاحها.

ومع ذلك، فليست جميع الدول تستسلم. قد يفكر بعض هذه الدول في أنه مادامت آثار الهجمات عبر الإنترنت مؤقتة وصعبة، فإن بإمكان نظمها تجاوز المناوشات الأولية والتعافي لمواجهة الجولات اللاحقة. ولذلك فهي تسعى وراء التقنية العالية، وتتجاهل إظهار إمكانية أن الحملات العسكرية ذات التقنية العالية يمكن أن تستمر أياماً وليس شهوراً أو أعواماً. وثمة استراتيجية مضادة أكثر دقة تتمثل في شبْك آلات القتال في الحرب (المصمَّمة لعدم الارتباط بالإنترنت) وعدم تشبيك الأشخاص؛ فالعزل يتفادى بعض نقاط الضعف المزعجة الناشئة عن الأخطاء البشرية (ولاسيما الأخطاء المرتبطة بعملية التحقق، مثل كلمات المرور والرموز). وإلا فإنهم ببساطة ينأون بأنفسهم عن الحرب القائمة على الشبكات ويخلصون إلى أنهم تجنبوا مخاطر الوقوع في شرك الاعتماد على التقنية.

من غير الواضح ما إذا كان بإمكان التلويح بقدرات الهجوم عبر الإنترنت أن يكبح حماس الأعداء المحتملين للحرب. قد تشعر بعض الدول أن لديها اختياراً محدوداً، بينما

ترى دول أخرى أن بإمكانها أن تنجح حتى إن أخفقت نظمها ذات التقنية العالية. ومع ذلك قد تُسقط دول أخرى من حسابها هذه الإمكانية تماماً، معتقدة أن نظمها - عندما تُدعى للحرب - سيتم فصلها عن بقية العالم. وأخيراً، فإن الجهة المستهدَفة يمكن ببساطة ألا تصدق أن لديها نقاط ضعف، لا في وقت السلم، وبالتأكيد ليس وقت الحرب. إن المضي إلى الحرب يتطلب التغلب على العديد من المخاوف الكبرى، وقد تكون الأشباح الرقمية ببساطة مصدراً آخر من مصادر هذه المخاوف.

تجدر ملاحظة الآثار غير المرغوبة التي تجعل حتى بعض الأطراف الثالثة تعتقد أننا غزونا نظمهم. إن جميع المؤسسات العسكرية الأخرى يمكن أيضاً أن تبتعد عن المصادر الأجنبية لوسائل معالجة العمليات المنطقية (سواء كانت برامج أو أجهزة)، وقد تُضاعِفُ جهودها لزيادة قدراتها الإنتاجية المحلية، أو تقوم - بدلاً من ذلك - بالضغط على مورديها لتسليم شيفرة المصدر مع الأجهزة، وهذا أمر سلبي إذا كان المورّد شركة أمريكية. ولن تنتهي المشكلة إذا تبيَّن أن التهديد لا ينجح. فالدول التي تتأكد من وقوع هجوم على نظمها العسكرية توجِّه اللوم إلى الولايات المتحدة الأمريكية على أي إخفاقات عسكرية، حتى من دون إثبات تورط الولايات المتحدة في ذلك. وبالمقابل، قد يتم اتهام الولايات المتحدة بالتآمر مع دولة مارقة إذا لم تصب أجهزتها بالتعطل والإخفاق؛ لأن هذا لا يعني سوى أن الولايات المتحدة تغاضت عن تصرفات تلك الدولة المارقة.

التلويح بقدرات الهجوم عبر الإنترنت في مواجهة نووية

هل ثمة ظروف يمكن أن تلوّح فيها الولايات المتحدة الأمريكية بشكل مفيد بأنها ستتدخل في الأسلحة النووية لدولة مارقة، وتنزع بالتالي فتيل مواجهة نووية؟ لنفرض أن دولة مارقة لديها عشرات الأسلحة التي يمكن أن تؤذي جاراتها، ولكن ليس الولايات المتحدة. ولنفرض أيضاً أن الولايات المتحدة تملك قدرات في الحرب عبر الإنترنت لا تتمتع الترسانة النووية للدولة المارقة بمناعة أكيدة ضدها. وإذا ما كان استعداد تلك الدولة المارقة للمضي إلى حافة الهاوية أكثر من استعداد الولايات المتحدة، فقد لا يتم

ردعها تماماً بالتهديد الأمريكي برد فعل مدمر تجاه استخدامها للأسلحة النووية. ونحن نفترض كذلك أن الدولة النووية المارقة تهدد بأنه إذا تجاوزت الولايات المتحدة "خطها الأحمر" فيمكن أن ترد بضربة نووية.

في البداية نصوغ نموذج مواجهة بين دولتين، ثم نأتي بدولة صديقة ثالثة تتصرف الولايات المتحدة نيابة عنها.

والسؤال هو: أيهما أشد حقداً وعناداً: الولايات المتحدة المصممة على تجاوز الخط الأحمر، أم الدولة المارقة المصممة بالدرجة نفسها على الرد بأسلحة نووية؟ وإذا استطاع أحد الجانبين إضافة ما يكفي من الثقة إلى استعداده للاستمرار في الضغط، فقد يشعر الجانب الآخر بأن الجانب الأول لن يتنازل، وسوف يعترف منطقياً بأن الاختيار هو بين الاستسلام والكارثة. وكلما زادت الدلائل على أن الجانب الآخر يمكن أن يستسلم، ازداد الحافز لدى الجانب الأول للثبات، مما يجعله يبدو أكثر عناداً تجاه الطرف الآخر.

يتمثل الهدف من التلويح بسلاح الحرب عبر الإنترنت في تهديد الطرف الآخر لمنعه من استخدام قدراته النووية في إحدى الأزمات. وهذا الهدف أقل من أن يجعل الطرف الآخر تساوره الشكوك في قدراته النووية (وإن كان ذلك عاملاً مساعداً)، ومع ذلك، فهو يعطي انطباعاً بأن الولايات المتحدة ستمضي في الضغط لسببين؛ إما لأن أسلحة الدولة المارقة لن تكون فعالة، أو لأن الدولة المارقة ستستجيب لتهديد الملوّحين بالهجوم (التي تؤكدها قدرات الردع بالطبع) وتستسلم. لاحظ أن المنطق ينجح حتى إذا كانت الدولة المستهدَفة تؤمن بأن ثقة الجهة الملوِّحة بالهجوم ليس لديها أساس في الواقع (كأن تكون القيادة والسيطرة النووية لديها صلبة وثابتة). ولا تحتاج الدولة المارقة سوى للاعتقاد بأن الدولة الملوّحة تؤمن بأنها تستطيع التصرف وتملك الحصانة والإفلات من العقوبة، لتخلص من ذلك إلى أن الاختيار هو بين الكارثة والاستسلام. وبالنظر إلى أنه يتعذر اختبار قدرات الحرب عبر الإنترنت بالطريقة نفسها التي يتم بها اختبار القدرات المضادة للصواريخ، فإن الدولة المارقة قد تخلص إلى أن الثقة لدى الجهة الملوّحة غير مضمونة، وبالتالي، فإن مثل هذه الثقة ينبغي ألا تكون موجودة؛ ومن ثم فلا وجود لها. ولكن ذلك قد يكون أيضاً مجرد تفكير مبني على التمني من جانب الدولة المارقة.

إذا أدى التلويح بالتهديد بهجوم عبر الإنترنت إلى إيجاد مأزق للدولة المارقة مؤداه "إما استخدام السلاح النووي وإما فقدانه" بحيث يدفعها إلى استخدامه، فإن هذا التلويح يمكن أن يعود بنتائج عكسية على الولايات المتحدة الأمريكية. ولكن ينبغي ألا يحدث ذلك، ويرجع ذلك عموماً إلى أنه ليس تهديداً بما سيحدث بل بما حدث بالفعل؛ فقد تم استغلال نقطة الضعف. لكن التلويح بقدرات الحرب عبر الإنترنت، وبخاصة إذا كانت محددة، يجعل من الصعب استخدام مثل هذه القدرات؛ لأن التلويح على الأرجح سيقنع الجهة المستهدفة بمضاعفة جهودها إما لاكتشاف نقطة الضعف المستغَلّة أو الالتفاف حولها (نقطة الضعف التي مكنت الولايات المتحدة الأمريكية من تحييد التهديد النووي). فالتلويح بالقدرات يؤدي إلى التضحية بالقدرة على إدارة حرب مقابل القدرة على إدارة أزمة.

يتمثل أحد العناصر المكنة لعملية التلويح في إيصال رسالة مفادها أنه ستتم ملاحظة أي طلقة نووية أخفقت [كالضغط على زر نووي]، والرد عليها حتى إذا كان الإخفاق غير ظاهر للمراقبين الخارجيين. وإلا فإن الدولة المارقة قد تفكر في أن الإخفاق بلا تكلفة، وأن النجاح، في حين يحتمل أن يكون باهظ التكلفة، يدل على الأقل على أنها جادة. أما إذا لم يكن الإخفاق الذي تم إحداثه ظاهراً (مثل أن يتم ضغط زر دون أن يحدث شيء)، فهل بإمكان الولايات المتحدة الانتقام لعمل تمت محاولة القيام به ولم يلاحظه سواها؟

بمجرد أن تصبح الأطراف الثالثة [الحليفة للولايات المتحدة] في وضع يسمح لها بالاعتراض على الأعمال العسكرية الأمريكية، فإن بإمكانها تعقيد استخدام التلويح. وعلى الرغم من أن الأطراف الثالثة يمكن أن يكون لديها روح عدائية ضد الدولة المسلحة نووياً، وبالتالي استعداد أكبر لرؤيتها ذليلة مهانة، ومرتدعة بلا ريب، فقد يصيبها الفزع من الخدعة المدعومة بالحرب عبر الإنترنت. أولاً، ستكون هي ومواطنوها عرضة لمخاطر جمة بسبب وجودهم ضمن نطاق الأسلحة النووية للدولة المارقة. ثانياً، ستكون معرفتها محدودة بقدرات الحرب عبر الإنترنت الأمريكية، ومن ثم ستكون أقل وثوقاً بفاعلية هذه القدرات من الثقة (المفترضة) لدى الولايات المتحدة الأمريكية. قد تتصور الدولة المارقة أنه لا داعي لأن تحمل الولايات المتحدة على الإذعان أو التردد إذا كانت تستطيع إرهاب الأطراف الثالثة التي تحتاج الولايات المتحدة إلى توافقها أو تعاونها في الأعمال العسكرية.

قد تحتاج الولايات المتحدة الأمريكية إلى خيارات لإقناع الطرف الثالث بأنها تستطيع الصمود باعتبار أن قدراتها الحربية عبر الإنترنت، بين أمور أخرى، ستسهم في تحييد التهديد النووي وتعطيله. يمكنها القول: "ثقوا بي في ذلك" وإلا! ولكنّ رداً أمريكياً يتجاوز طلب الثقة قد يتعين أن يكشف عن تفاصيل قدرات الحرب الأمريكية عبر الإنترنت أكثر مما ترتاح الولايات المتحدة إلى الكشف عنه الآن. فحدوث أزمة قد يجعل هذا الكشف مثيراً للإشكالات؛ فعلى الرغم من أن الصمود يمكن أن يستدعي من القوى المؤيدة للأمريكيين أن تثق بقدرة الولايات المتحدة الأمريكية على إبطال تهديد نووي، فإن أولئك القلقين من الإقدام على مثل هذه المخاطرة الهائلة، أو المشككين في القدرة على الحرب عبر الإنترنت، أو خصوم الولايات المتحدة داخل حكومة الطرف الثالث، لديهم كل الدوافع لإلقاء ظلال من الشكوك على الاقتراح، أو حتى تسريب المعلومات التي تم ائتمانهم عليها. (بالمناسبة، ينطبق منطق مماثل إذا كان الطرف الثالث الصديق داخلياً، مثل الكونجرس الأمريكي وأصحاب الرأي وعامة الشعب). وقد يكون من مصلحة الدولة المارقة أن تفترض ضمناً أن قدرات الحرب عبر الإنترنت (وليس الثقة في تأثير الردع للأسلحة النووية) هي الأساس الرئيسي للموقف الثابت الذي اعتمدته الولايات المتحدة. ويمكن أن يضغط هذا على الولايات المتحدة لإظهار ما يمكنها فعله.

خلاصة

من شأن التلويح بقدرات الهجوم عبر الإنترنت أن يؤدي إلى ثلاثة أمور: إعلان القدرات، والإيحاء بإمكانية استخدامها في ظرف معين، وإيضاح أن مثل هذا الاستخدام سيسبب الأذى بالفعل. في حقبة المواجهة النووية الأمريكية - السوفيتية كانت دلالات الاستخدام هي الأكثر وروداً؛ فقد كان امتلاك هذه الأسلحة واضحاً للعيان، وكانت عواقبه مفهومة جيداً، غير أن هذا لا ينطبق على أسلحة الفضاء الإلكتروني. فالحيازة على الأرجح غير واضحة، والقدرة على إلحاق أضرار خطيرة تظل موضع جدل، وحتى إذا تمت البرهنة عليها، فما كان ينجح أمس لا ينجح اليوم، غير أن الصعب لا يعني المستحيل.

قد تكون الدعاية لقدرات الحرب عبر الإنترنت مفيدة، وقد تساند استراتيجية الردع، كما قد تردع الدول الأخرى عن الأذى التقليدي، أو حتى عن الاستثمار في قدرات إلحاق الضرر. ولعلها تحدّ من ثقة الطرف الآخر في صدقية معلوماته، أو قيادته وسيطرته، أو منظومات أسلحته. وقد تفيد في المواجهات النووية ببناء الوسيلة التي تقنع بقية الدول بأن الذي يلوّح بالهجوم جاد في ذلك، وبذلك تقتنع بالإذعان.

ومع ذلك، فإن إثبات مثل هذه القدرات ليس بالأمر السهل، حتى إذا وُجدت؛ فقدرات الفضاء الإلكتروني لا تظهر إلا في علاقتها مع هدف محدد، ويجب معرفة نطاقه ومداه كي يتم فهمه. وبإمكان محاربي الفضاء الإلكتروني إيضاح قدرتهم على اختراق النظم، ولكن اختراق هذه النظم لا يضاهي تعطيلها من خلال طرق مفيدة. وبما أن الهجمات عبر الإنترنت تُعدُّ في الأساس أسلحة أحادية الاستخدام، فإنها تتضاءل مع استعراضها. وقد يكون من الصعب إقناع أصدقائك بأن لديك مثل هذه القدرات عندما تكون الشكوك في مصلحتهم.

علاوة على ذلك، فإن التلويح يمكن أن تكون له نتائج عكسية. ذلك أن الترويج للقدرة على الرد في الفضاء الإلكتروني، يمكن أن يوصل رسالة مفادها الابتعاد عن العنف. وقد يؤدي ادّعاء القدرة على تغيير الواقع إلى إقناع الآخرين بتوجيه اللوم إلى المدّعي إذا كان الواقع غير ملائم. أما التدخل في القيادة والسيطرة لدى الآخرين فيمكن أن يسمح لهم بتبرير قواعد الاشتباك التي تجعلهم يتخلون عن مسؤوليتهم عن تابعيهم، كما أن تأكيد القدرة على إحباط نظم نووية مضادة يمكن أن يدفعهم إلى تسمية ما يتصورونه خدعة.

هل يتعين على الولايات المتحدة الأمريكية أن تُشعر العالم بأنها تمتلك قدرات الهجوم عبر الإنترنت، وبأنها تعرف كيف تستخدمها؟ ليس ثمة حكمة واضحة في مثل هذا المسار. فلا توجد سوى أدلة ضئيلة على أن الآخرين يتصرفون؛ لأنهم لا يصدقون أن الولايات المتحدة تملك قدرات عبر الإنترنت أو تستطيع تطويرها. وبالمقابل، تعتمد المكاسب من

مثل هذا التلويح بهذه القدرات على السياق، ويمكن أن تكـون مثـيرة للمـشكلات حتـى حينئذ.

إن التلويح بالهجوم عبر الإنترنت ينطوي على أمور مـشجّعة وعـلى مخـاطر أيـضاً، في الحالتين التقليدية والنووية على حد سواء. ولا ضير في التفكـير الجـدي في طـرق تـستطيع الولايات المتحدة الأمريكية من خلالها تعزيز قدرتها على استغلال ما يراه الآخرون قدرات وطنية. ومن المؤكد أن فيروس ستكسنت قد أقنع آخرين بأن الولايـات المتحـدة تـستطيع فعل الكثير من الأمور المتطورة في الفضاء الإلكتروني (بغض النظر عما إذا كانت الولايات المتحدة قد ساهمت بشكل عملي في ستكسنت أم لا). وسوف يتطلب هذا الجهد كثيراً مـن التحليل والتخيل؛ لأن الخيارات المختلفة التي عُرضت في هذه الدراسة لا يعتـبر أي منهـا ناجحاً بشكل واضح. ذلك أن التلويح خيار قد لا يـنجح أيـضاً، فهـو لـيس ترياقـاً لكـل العلل. ومن المستبعد أن يساعد التلويح على نجاح الردع إذا كانت عناصر الردع الأخـرى (إرادة شن الحرب أو القدرة على إلصاق التهم بالنسبة إلى الخطـوط الحمـراء المرسـومة في الفضاء الإلكتروني) ضعيفة.

الفصل الأول

لا استعراضات في عيد العمال

الخلفية والهدف

كانت العروض العسكرية للمقاتلين والأسلحة التي تجوب الشوارع الرئيسية في المدن أسلوباً تدلل الدولة من خلاله على قدرتها على خوض الحرب. ومن المؤكد أن قدرات الحرب عبر الإنترنت تناقض مثل هذا العرض؛ فكوادر خبراء الحاسوب الذين يسيرون وحواسيبهم المحمولة في حقائب على ظهورهم لا يشيعون الرهبة والمهابة نفسها في النفوس.

إن العجز عن إظهار نقاط القوة يشير إلى مأزق أكبر في الحرب عبر الإنترنت؛ فليس الغرض من وجود القوات المسلحة الأمريكية هو القتال وكسب الحروب فحسب، بل الردع والحيلولة دون وقوع هذه الحروب أيضاً، أي إقناع الآخرين بعدم شنها (أو حتى الإعداد لها). ولهذا الغرض فإن من المفيد إيضاح أن القوات الأمريكية ستقوم دوماً على الأرجح بتدمير الذين يُقْدمون على محاربتها، سواء كان التدمير في هيئة سحق القوات العسكرية أو إنزال الأضرار بالمجتمع. ولعل الولايات المتحدة تأمل من خلال ذلك ردع الآخرين عن مهاجمتها أو مهاجمة مصالحها الحيوية، سواء بالحركة أو من خلال الفضاء الإلكتروني. ولعلها تأمل حتى أن تصرف الآخرين عن تطوير قدرات رقمية تكون بصورة خاصة عرضة للهجوم عبر الإنترنت. وعلى الرغم من أن استعراضات الأول من مايو [الذي يصادف عيد العمال] تتصف بشيء من العروض الكاريكاتورية، فإن من المنطقي أن تستقصي أي دولة قدرات خصومها المحتملين قبل السعي وراء استراتيجياتها السياسية-العسكرية، غير أنه من الصعب فحص قدرات الحرب عبر الإنترنت.

لِمَ ذلك؟ لا أحد يشك في ما سيحدث لو أن قوة مسلحة نووية ألقت بسلاحها الهائل على مدينة، على الرغم من أنه لم يتم ضرب أي مدينة بقنبلة نووية منذ عام 1945. والقوانين الطبيعية واضحة وهي تنطبق في أي مكان، ولكن لا أحد يعلم تماماً أو حتى بشكل تقريبي ما سيحدث إذا تعرضت دولة لهجوم شامل عبر الإنترنت على الرغم من زيادة النشاط المعادي في الفضاء الإلكتروني الذي لا تبدو ثمة علامات على نقصانه. ولسبب ما، لم يقع مثل هذا الهجوم.

إن النظرية أيضاً تثبط التوقعات الجيدة المسلم بها. فالنظم، أولاً، عرضة للهجوم بقدر ما يوجد فيها من أخطاء يمكن استغلالها ولا يعلم بها أصحابها، أو أنهم ببساطة تجاهلوها. ثانياً، حتى إذا نجح الهجوم عبر الإنترنت فإن الضرر الذي يحدثه من شأنه أن يكون متناسباً مع الزمن اللازم لتعافي النظام الذي تعرَّض للهجوم، وهو أمر لا يستطيع المُدافع ولا المهاجم التنبؤ به بسهولة. ثالثاً، تُعتبر القدرات الوطنية في مجال الحرب عبر الإنترنت سراً مصوناً بشدة.

بعد أن أمضت الدول الكثير من الوقت، وتحمَّلت العناء الشديد في تطوير قدراتها في الحرب عبر الإنترنت، لا يوجد لديها ما تعرضه عن جهودها إلى أن تمضي لخوض حرب عبر الإنترنت. وعلى الرغم من أن بعض القدرات اللازمة للحرب عبر الإنترنت هي نفسها المستخدمة للتجسس عبر الإنترنت، فإن بعضها الآخر ليس كذلك. إن تخريب النظم يتطلب جهداً لفهم وضعيات تعطيلها، كما يتطلب إبقاؤها معطلة وغير قادرة أن يتم إدخال شيفرة أو رمز في الشبكات المستهدفة بطرق تجعل من الصعب القضاء عليها. أضف إلى ذلك أن النظم المستهدفة بالتجسس (مثل شبكات البريد الإلكتروني) تختلف كثيراً عن النظم الأكثر صعوبة التي تدير بنية تحتية حساسة أو آلات حربية.

وكون التلويح بمصداقية قدرات الهجوم عبر الإنترنت ليس سهلاً، لا يعني عدم إمكانية التلويح بها مطلقاً. وسوف تسعى هذه الدراسة إلى استقصاء الطرق التي يمكن بها استخدام قدرات الحرب عبر الإنترنت بهذا الشكل، والعقبات التي تعترض ذلك، وبعض المخاطر التي ينطوي عليها ذلك، والقيود التي تحد من توقعاتنا.

ما هو التلويح؟

إن التلويح بسلاح يدل على ماهية هذا السلاح، وكيفية استخدامه.[1] ويمكن أن يكون التلويح ضمنياً، بحيث يترك للآخرين أن يحددوا انعكاسات استخدامه. أو يمكن أن يكون صريحاً، حيث يختار الملّوح بالتهديد السياق والتوقيت ليرسل رسالة.[2]

يتم عموماً التلويح بالقدرات لصياغة، أو على الأقل لتعزيز، تقديرات الدول الأخرى للمخاطر التي تواجهها إذا عارضت الجهة الملوّحة بالتهديد. أما بالنسبة إلى الفضاء الإلكتروني فتختلف التقديرات اختلافاً كبيراً؛ ذلك أن قدرات الهجوم عبر الإنترنت هي دائماً قدرات ضد نظم محددة، وتختلف الدول في نوعية النظم الموجودة بحوزتها، وفي مدى أهميتها، ومدى الأمن الذي تتمتع به.

وبما أنه ليس من دولة بلغتها أخبار فيروس ستكسنت ستصدق حقاً أن الولايات المتحدة الأمريكية تفتقر إلى قدرات هجومية عبر الإنترنت، وبما أن عديدين يجادلون دفاعاً عن تغليب الجريمة في ذلك،[3] فلعل قدرات الحرب عبر الإنترنت لدى الولايات المتحدة قد ثبطت الآخرين بالفعل عن إلحاق الأذى بها في الوقت الحاضر،[4] إذ بإمكان الأسلحة وحدها فعل ذلك. ففي عام 1932 (قبل أن يصبح لدى ألمانيا سلاح طيران)، أقنع ستانلي بالدوين البرلمان البريطاني بعدم التدخل بسرعة كبيرة في الشؤون الأوروبية بحجة أن خصماً خطيراً يمكن أن يستخدم القوة الجوية لإحداث أضرار عظيمة لبريطانيا العظمى: «سوف تقوم القاذفة دائماً بالاختراق».[5]

فلماذا التلويح بالهجوم عبر الإنترنت؟

- يتلخص أحد الأسباب ببساطة في إطلاق تهديد، إما بشكل محدد (افعل هذا وسوف نقوم بتنفيذ هجوم عبر الإنترنت) أو بصورة عامة (افعل هذا وسوف نرد بقدرات تشمل هجوماً ممكناً عبر الإنترنت).

- وثمة سبب آخر يتمثل في التصدي لتهديد، سواء كان صريحاً أو ضمنياً، وهذا يشبه إعلان قدرة على الدفاع الصاروخي البالستي بعد إعلان الطرف الآخر امتلاكه قدرة

صاروخية بالستية، حيث تؤدي الحرب عبر الإنترنت دور سلاح موجه في القيادة والسيطرة الصاروخيتين. وقد يتم مثل هذا الإعلان للتهوين من أمر التهديد، لطمأنة النفس والحلفاء، وبذلك يتم إضعاف القوة الرادعة للتهديد، فإذا كان التهديد الكامن وراء ذلك ردعاً مضاداً (إذا أطلقتم صاروخاً فسوف نرد بصاروخ في المقابل)، فيمكن التلويح بقدرات الهجوم عبر الإنترنت لتعزيز الرادع الأصلي (أجل، ولكن صاروخكم سيخطئ هدفه، وبالتالي سنتجاهل تهديدكم). ويساعد مثل هذا التلويح على إبراز الثقة.

- يمكن أن يؤدي التلويح بقدرات الهجوم عبر الإنترنت إلى تحذير الآخرين من السعي وراء قدرات تعتمد على النظم الرقمية بصورة عامة، والشبكات بصورة خاصة. وكبديل لذلك التهديد، يمكن التلميح إلى أن المعلومات التي يستخدمها الأعداء المحتملون لاتخاذ قرارات عملياتية أو حتى استراتيجية يمكن إفسادها ومن ثم تكون غير موثوقة. ولا داعي لأن يكون التهديد استباقياً (إن فعلتم كذا ...)، فبإمكان الملوّح أن يلمّح إلى أن الهجوم لإفساد البيانات قد وصل هدفه المنشود، ما يعني أنه لا يمكن حتى الثقة بالبيانات الحالية.

وسوف تعتمد مصداقية التهديد بالهجوم عبر الإنترنت على سجل إنجازات دولة ما في الفضاء الإلكتروني، مقروناً بسمعتها العامة في مجال التقنية العسكرية، ومدى احتمال أن تستخدم مثل هذه القدرات عندما تدعو الحاجة. وأخيراً، فإنه كما أن تقنيات الفضاء الإلكتروني واعتماد الدولة المستهدفة على الإنترنت يتطوران، فإن ذلك ينطبق أيضاً على فاعلية مثل هذه التهديدات.

التلويح والردع: ملاحظة تحذيرية

يتمثل أحد الأسباب التي تدعو دولة ما للقول أو للتلميح بأنها تمتلك قدرات حربية هجومية عبر الإنترنت في تزويد سياسة الردع لديها بأسنان [أي قوة فعلية].[6] وكقاعدة عامة، فإنه كلما كانت قدرات دولة على الضرب أكبر، كانت العواقب أكبر في حال تجاوز

الدول الأخرى الخطوط المرسومة، ومن ثم انخفاض احتمال أن تتجاوز تلك الدول هذه الخطوط (على الأقل إلى المستوى الذي تخاف عنده الدول الأخرى على سيادتها وتسعى لتحجيم الدولة؛ لأنها تشكل تهديداً كبيراً). ومع ذلك، فإن الردع يتطلب بعض الوضوح لتحديد الخطوط الحمراء، ومدى استعداد تلك الدولة لتنفيذ تهديدها وبأية وسائل. وبدون مثل هذا الوضوح فقد يترك التهديد أثراً عكسياً لما هو مقصود.

لذلك، فإن الكثير يعتمد على ما تستخلصه الدول الأخرى بشأن الدافع وراء التلويح بقدرات الحرب عبر الإنترنت، وتوقيت ذلك التلويح. فإذا كانت الدولة التي تصدر عنها التهديدات صريحة في أنها ستستخدم وسيلة الحرب عبر الإنترنت لتنتقم في حال تجاوز خطوط حمراء معينة (افتراضاً، وليس بالضرورة، في الفضاء الإلكتروني)، فإن دور التلويح يكون واضحاً إلى حد ما؛ وهو إضفاء قيمة على التهديد. غير أن التوقيت قد يثير تساؤلات، ولاسيما إذا لم تعلم دول أخرى أي شيء جديد عن قدرات الدولة الملوحة بالتهديد (والتي افترضوا دائماً أنها موجودة) ولكنهم غير متأكدين بشأن الأسباب التي دفعت الدولة المهدِّدة إلى الاعتقاد بضرورة التصريح بهذه النقطة. فالسياق مهم، ولعل التلويح بالقدرات لتأكيد تهديد قد تم إعلانه (أو خط أحمر قد تم تحديده أو إعادة رسمه) يثير بضعة تساؤلات عن التوقيت، غير أن التلويح بقدرات فجأة يمكن أن يثير المزيد من هذه التساؤلات. فقد يراه البعض نوعاً من الخداع، كمحاولة للتظاهر بالشجاعة عند اكتشاف أن القدرات عبر الإنترنت لا تؤثر في نفوس الآخرين لسبب وجيه وهو أنها ليست بذلك التأثير.

لكن إذا لم تقم الدولة المبادِرة بالتهديد بالتصريح أو التلميح بقوة بأن خيارها في الانتقام يكمن في الفضاء الإلكتروني، فإن الدول الأخرى قد تتساءل عما يدفع هذه الدولة إلى تأكيد قدراتها الانتقامية في ذلك النطاق. صحيح أن الإجابة قد تكون بريئة: قد يكون ثمة صراع بيروقراطي تم حله، أو أن قدرة جديدة في الهجوم عبر الإنترنت يمكن اعتبارها ناضجة. لكن الدول غير المعنية بمثل هذه التوضيحات يمكن أن تستخلص أن التلويح بقدرات الهجوم عبر الإنترنت يهدف إلى إرسال رسالة بأن اللجوء إلى ردود أشد عنفاً هو

أمر غير مطروح. ولذلك، فإن الدول التي لا تخشى القدرات عبر الإنترنت (ربما لأن قواتها العسكرية أو اقتصاداتها لا تعتمد على التقنيات الرقمية على الإطلاق) قد تستنتج أن بإمكانها الاسترخاء، وقد تكون بالتالي أقل تأثراً بالردع.

تنظيم هذه الدراسة

بعد ذكر هذه التحذيرات، فإن بقية الدراسة تحلل عواقب التلويح بقدرات الهجوم عبر الإنترنت، حيث أقوم بدراسة أربعة أهداف منفصلة للتلويح بقدرات الهجوم عبر الإنترنت: تثبيط العمليات العسكرية، وصرف الدول عن الاستثمار في القدرات في مجال الشبكات، والسماح للولايات المتحدة الأمريكية بالتصدي للدول المارقة المسلحة نووياً، وكبح العدوان النووي غير المستفَز.

يتناول الفصل الثاني التلويح بصورة عامة: ماذا تستطيع الدول فعله لإثبات الدعاوى بأنها تملك مثل هذه القدرات، أو على الأقل دعم دعاواها؟ وكيف؟ وضد من؟ وكيف يمكن استخدامها للحد من رغبة الدول الأخرى في تنفيذ عمليات، أو حتى الاستثمار في قدرات عملياتية معينة، وفي حسابات التهديد وإشكالياته؟

أما الفصل الثالث فيتناول كيفية التلويح بأسلحة الفضاء الإلكتروني في مواجهة نووية. ومن الواضح أنه عند مواجهة التدمير، فإن من غير المرجح أن يسجل خطر التعرض للاختراق نسبة عالية، لكن الاستخدام العملياتي للحرب عبر الإنترنت لإحباط دورة القيادة والسيطرة النوويتين للخصم يمكن أن يكون له دور مهم.

أما الفصل الرابع فيلخص الأفكار الثاقبة الرئيسية لهذه الدراسة.

الفصل الثاني

الآثار العامة للتلويح بقدرات الهجوم عبر الإنترنت

إن التلويح بقدرة لا يمكن أن تُعرض للمراقبة والفحص، ولا يمكن استعراض أي تفصيل منها دون إبطالها بسرعة، ينطوي على تحديات غير قليلة. في هذا الفصل أقوم ببحث طرق مختلفة في التصدي للتحديات، مستنتجاً أنه على الرغم من أن كل طريقة لها مزاياها، فإنها جميعاً ليست مُرضية. ولذلك، فإن هذا الفصل، حسب التسلسل، يناقش كيف يمكن أن يشير اختراق النظام إلى القدرات الهجومية عبر الإنترنت؟ وكيف يمكن إحداث الخوف واستمراره من أنه قد حصل الاختراق بالفعل؟ وكيف أن المخاوف من الاختراق يمكن أن تؤثر في السلوك العملياتي للخصم، بل حتى في استثماراته الدفاعية؟ وبعد ذلك، يتفحص بعض العواقب المترتبة على استخدام الهجمات عبر الإنترنت كوسيلة إكراه، ويبحث في طرق يمكن أن يؤدي فيها التلويح إلى نتائج عكسية، ويُختتم الفصل ببحث السياسات الحالية المرتبطة بشرعنة الحرب عبر الإنترنت.[1]

أي دور للتلويح؟

بما أن إمكانية حدوث الهجمات عبر الإنترنت تنجم عن نقاط الضعف لدى الجهة المستهدفة مقرونة بقدرة المهاجم على استغلالها، فهل الأثر المنشود للتلويح بقدرات الهجوم عبر الإنترنت هو أن تبدو قوياً أو جعل الطرف الآخر يبدو بلا حول ولا قوة؟ بالطبع، يمكن أن يكون الجواب كلا الأمرين، وكلاهما يمكن أن يكون مفيداً، لكن إذا كان التلويح جزءاً من حملة اتصالات استراتيجية شاملة فقد يساعد على اتخاذ قرار بشأن ما ينبغي التركيز عليه في مثل هذه الحملة.

إن الظهور بمظهر القوة هو الخيار الأكثر فاعلية؛ فهو يولد الحذر لدى الخصوم الحقيقيين والمحتملين، وليس من الضروري تكرار الاستعراض لكل خصم. ويسهم

الظهور بمظهر الدول الكبيرة أيضاً في صرف المهاجمين عن دولة نحو دول أخرى. وأخيراً ينطوي ذلك على هالة من المجد، فالنجاح ينعكس بشكل إيجابي على مصادر أخرى للقوة الوطنية.

لكن التركيز بدلاً من ذلك على الكشف عن نقاط الضعف لدى دولة أخرى له قيمته ومزاياه أيضاً؛ فهو يسهم في ردع الدول المزعجة بتذكيرها بمواطن ضعفها، كما أنه يُبعد الاتهامات بالترويج للذات (انظروا كم أنا قوي) من خلال تحويل التركيز نحو الآخرين. ومع ذلك، فإن الدولة التي يظهر لأحد المهاجمين أنها ضعيفة ومنكشفة لعدوان، قد يكون من المفترض أنها ضعيفة أمام آخرين أيضاً. وحتى إذا بادرت الدولة إلى الانتقام، فإن أنظمتها ستبقى عرضة للهجوم ويُنظر إليها على هذا الأساس.

ثمة هدف آخر لعله يصرف الولايات المتحدة الأمريكية عن الهجوم على أي جهة. ففي الاقتصاد المعولَم قد يؤدي شن هجوم عنيف عبر الإنترنت ضد مؤسسات أجنبية إلى إلحاق الأذى بالولايات المتحدة في مصالحها الاقتصادية؛ بصورة مباشرة، إذا كان الاقتصاد الأمريكي يعتمد على خدماتها المعلوماتية، وبصورة غير مباشرة، من خلال الآثار في أسعار الصادرات وتوافر المواد. وقد يكون لهذا الهجوم عواقب سياسية؛ إذ إن الحرب عبر الإنترنت تقضي على الثقة، بينما تسهم الهجمات الناجحة في إرباك حكم القانون. إن اتخاذ وضع يرمي إلى منع حدوث حرب عبر الإنترنت بصورة عامة، وليس على الولايات المتحدة الأمريكية فحسب، يتلاءم ورواية السياسة الحالية للولايات المتحدة بأن المشكلات الأمنية في الوقت الحاضر هي نتيجة التصرفات المارقة من قبل الدول المارقة.

هل يعبّر الاختراق الناجح بما يكفي عمّا يمكن أن تفعله الحرب عبر الإنترنت؟

إن أوضح طريقة للتدليل على القدرة على القرصنة على نظام شخص آخر تكون في الواقع في تنفيذ ذلك، وترك أثرٍ، على شكل بطاقة دعوة (مثلاً: كيلْروي كان هنا Kilroy was here). ولا ضرورة لأن يكون الأثر واضحاً للجمهور، ولكن ينبغي على الأقل أن يكون واضحاً لمديري النظام. فإذا أمكن تكرار الهجوم متى شاء المرء، أو إذا كان يمكن

جعل الاختراق غير قابل للإزالة، فقد تضطر الجهة المستهدَفة إلى الاعتقاد بأن قدرة الجهة التي قامت بالاختراق على الولوج إلى النظام متى شاءت تُعتبر أمراً حقيقياً. وهذا يضطر الجهة المستهدَفة إلى إعادة حساب ميزان قواها ضد مرتكب الهجوم.

يبدو هذا أمراً بسيطاً. لكنه في الواقع ليس كذلك، وذلك من خلال النظر إلى معظم الأشياء في الفضاء الإلكتروني. المشكلة الأولى هي ما إذا كان سيتم ملاحظة الأثر، أو بطاقة الدعوة، ويتم إبلاغ القيادة بوجوده. فإذا تُرك ببساطة لشخص ما ليعثر عليه، فالإجابة هي "لا". ومن المفارقات أنه كلما كان النظام أكثر عرضة للاختراق، كان مديرو النظام أقل حدة في الذكاء، في حال كون كل العناصر الأخرى متساوية. وهكذا، نجد أن اكتشاف الاختراق ونقله إلى القيادة يصبح أقل ترجيحاً. ولهذا السبب، فإن من الضروري أن يكون الأثر (أو بطاقة الدعوة) الذي يُترك واضحاً جداً. وربما يكون بالإمكان أن ترسل تلك البطاقة نفسها - إذا جاز التعبير - إلى البريد الإلكتروني لمديري النظام، على أمل أن يبلغوا القيادة. فإذا كان النظام المستهدَف موصولاً ببقية العالم - وبخاصة النظم الحساسة - فيمكن أن تصل مباشرة إلى البريد الإلكتروني لقيادة الجهة المستهدفة. ومن المفترض أن ينجح ذلك (ما لم يعتقد القادة أن الأمر خدعة من جانب خصومهم في الحرب عبر الإنترنت للحصول على مزيد من الموارد من أجل الأمن في الفضاء الإلكتروني). والعكس أيضاً ممكن. فإذا كان الإقرار بالاختراق مدعاة للإحراج ويعرِّض الوظائفَ، وفي بعض الدول، الأرواحَ للخطر، فقد يتم حذف مثل هذه الملاحظات أو التعليقات من قبل مديري النظام المحرجين. وإن الكشف عن سر لا سبيل لكشفه إلا بسرقته من ذلك النظام، يزيل مشكلة الحذف بعد انكشاف الحقيقة، غير أنه يبرز السؤال عما إذا كان من الممكن ألا تأتي المعلومات إلا من اختراق النظام (وليس من الجواسيس، مثلاً).

تتمثل الصعوبة الثانية في إثبات أن القدرة على اختراق نظام متى شاء المرء هو أمر يتصف بالأهمية. وإذا حدث - كما سبقت الإشارة إليه - أن كان اختراق مؤكد، حادثة غير متكررة، فقد تقنع الجهة المستهدَفة نفسها بأن باستطاعتها اتخاذ إجراءات لضمان استحالة تكرار حدوث ذلك، أو أن الضحية يمكن أن تتهاون إزاء قدرة المهاجم على البقاء في

النظام تحديداً؛ لأنها تجد الاختراق أقل كلفة من إعادة الضبط الشامل للنظام. ويضع مثل هذا التقييم بصورة آلية حداً أعلى لتأثير استعراض الهجوم عبر الإنترنت. أضف إلى ذلك أن فاعلية الاختراق لها علاقة وثيقة بحساسية النظام الذي يتم اختراقه. ويتطلب هذا معرفة أي النظم تعتبر حساسة وحيوية بالنسبة إلى الجهة المستهدَفة، واختراق أي واحدٍ منها سيكون مؤثراً. فإذا كانت القوة السياسية للجهة المستهدفة تعتمد على التشغيل الصحيح للنظم التي ليست معزولة إلكترونياً فحسب، بل هي مخفية أيضاً، فإن اختراق النظم الأقل شأناً قد يخلّف تأثيراً ضئيلاً على تلك الجهة. ويمكن ملاحظة أن اختراق نظام واستمرار البقاء داخله، يتطلب مجموعات متشابهة من المهارات، ولكن بتقنيات مختلفة. فالاختراق يتطلب معرفة نقاط الضعف، ويتطلب الاستمرار والمثابرة ومعرفة كيف يتم تجنب نظم كشف التسلل والنشاطات الغريبة في النظام.

تُرى، هل تسهم القدرة على اختراق نظام ما في إثبات القدرة على تخريب نظام؟ من منظور تقني: لا. وعلى النقيض من التأكيدات، فإن القدرة على قراءة الملفات لا تنطوي ضمناً على القدرة على كتابتها، وبالتالي تغييرها، تماماً مثل القدرة على مشاهدة فيديو نيتفليكس Netflix على حاسوب محمول، فإن ذلك لا يعني قدرة هذا الحاسوب على تحرير مثل مقاطع الفيديو هذه. إن تخريب نظام لا يتطلب اختراق حسابات مدير النظام (أو الحسابات المميزة) فحسب، بل أيضاً معرفة كيف تُسبِّب الإخفاق للنظام واستمرار ذلك رغم كل الخواص والمزايا المصممة لتحول دون ذلك. غير أنه من منظور سيكولوجي، لعل القدرة على اختراق نظام لا تثبت القدرة على تعطيله وتدميره، ولاسيما إذا كانت القيادة المستهدفة لا تميز الفرق بين الاختراق والتعطيل. فإذا جاء الاختراق (وهو انتهاك إذا جاز التعبير) بمنزلة صدمة، فإن المزيد من الانعكاسات يمكن أن يروع القيادة، بغض النظر عن مدى عدم وجود أساس تقني لمثل هذه الانعكاسات.

لكن تعطيل نظام يُعتبر تصرفاً أشد عدوانية وأكثر صعوبة من اختراقه؛ إذ يتطلب فهماً لسمة فشل وضعيات النظام. وكذلك الأمر بالنسبة إلى إيجاد الآثار الضرورية، فإنه يتطلب صياغة شكل الهجوم بحيث لا يستطيع مديرو النظام المستهدف اكتشاف النظام

"بسرعة كبيرة" وإصلاحه. ويتحدد تعريف "بسرعة كبيرة" بالضرورة حسب السياق. وقد يستمر الهجوم على إمدادات النظام أياماً أو أسابيع قبل أن يؤدي ذلك إلى شلل للسكان المستخدمين لهذا النظام. لكن هجوماً على منظومات صواريخ أرض-جو لا يُفترض به أن يعطل المنظومات سوى بضع دقائق أثناء حالة الطيران في الأجواء. ومع ذلك، فإنه من غير الواضح مدى إمكانية الإسراع بإعادة الأمور إلى الوضع الطبيعي، فتاريخ الهجمات عبر الإنترنت التي تستدعي إصلاحات عاجلة محدود، وتوثيق ضحايا مثل هذه الهجمات لايزال أقل، ولعل المهاجمين عبر الإنترنت (هنا وفي أماكن أخرى) قد سعوا إلى تقدير استجابات الخصم من خلال تحريض هجمات على نظمهم هم واختبار قدرة مديري نظمهم على استعادة وضع تشغيلها الطبيعي. وحتى إذا كان الوضع كذلك، فإن التحدي المتمثل في إيصال رسالة إلى آخرين بأن الهجمات يمكن أن تعطل نظمهم لفترات طويلة ليس بالأمر السهل. وقد تكون الجهة المستهدفة قادرة على تحديد الخلل الذي سمح بوقوع ذلك الهجوم ومن ثم إصلاحه واستعادة بعض الثقة بنظمهم. وإذا كان الأمر كذلك، فلكي ينجح تلويحهم بالهجوم، فلا بد من البرهنة على مثل هذه القدرات الهجومية عبر الإنترنت بصورة متكررة.

أضف إلى ذلك أن الخط الفاصل بين التلويح بقدرة ما واستخدامها، يمكن أن يصبح رفيعاً جداً. ومن المفترض أن هدف التلويح يتمثل في الحد من رغبة الآخرين في تحدي من يملك قدرات الهجوم عبر الإنترنت. لكن استخدام إحدى القدرات من شأنه أن يخلّف أثراً عكسياً؛ فهو يزيد رغبة الطرف الآخر في تحدي صاحب القدرة. إن من طبيعة الإنسان أن يرد الضربة. وفي الفضاء الإلكتروني، كما هو الشأن في وضعيات الصراع الأخرى، يمكن أن يعود التلويح بنتائج عكسية.

ثمة طريقة ممكنة للخروج من هذا المأزق، وتتمثل في استعراض القدرة على تدمير نظام شخص آخر من خلال البرهنة على القدرة على التلاعب به بطرق يمكن أن تخرِّبه بشكل ملحوظ إذا استمرت أو تم تنفيذها في سياقات أخرى. على سبيل المثال، البرهنة على وضع بقعة بيضاء فارغة على رادار أثناء العمليات العادية ينطوي ضمناً على القدرة

على وضعها هناك عندما يتتبع الرادار جسماً معادياً. كما أن القدرة على رفع حرارة عملية كيميائية لشخص ما درجة واحدة يمكن أن يدل ضمناً على القدرة على رفع درجة الحرارة بصورة تؤدي إلى إحداث ضرر خطير، بما في ذلك تدمير الأجهزة. قد يكون إحداث بقعة فارغة أو ذبذبة درجة الحرارة بمنزلة هجمات معادية، ولكنها ليست أعمالاً حربية. ومع ذلك، فإنها قد تكون كافية للإيحاء بأن التدخل في العمليات أو تدمير منشأة كيميائية - حيث يمكن اعتبارهما من أعمال الحرب - يقعان ضمن قدرات المهاجم. وتطبَّق التحذيرات المعتادة؛ إذ يجب نقل مثل هذه الاستعراضات إلى القادة، وتُعتبر مثل هذه الاستعراضات مقيِّدة للمهاجِم إذا أنتجت تصحيحات داخل النظم المستهدفة تعقّد التكرار. وبالنسبة إلى بعض النظم قد لا ينطوي أحد المعطيات ضمناً على القدرة على فعل أمور خطيرة كهذه إن كانت توجد تدابير احتياطية.

بث الخوف والغموض والشكوك

لقد أدت الأسلحة النووية إلى إثارة الرعب، ولكن لم يكن ثمة شك كبير أو غموض حول استخداماتها.[2] قد يكون الفضاء الإلكتروني على العكس من ذلك؛ أي غير قادر على بث رعب حقيقي بصورة مباشرة، بل قد يكون قادراً على إثارة شبح الشكوك والغموض، ولاسيما في عقول الذين يمكن أن يتساءلوا عما إذا كانت أنظمتهم العسكرية، ومن ثم، قواتهم المسلحة، ستعمل عند الحاجة إليها. ومن شأن هذا أن يسبب القلق إذا كانوا سيستخدمون قوة مشكوكاً في موثوقيتها. ولا داعي لأن تعتقد الدولة المستهدفة أنها ستخسر حرباً كان يمكن لها أن تربحها لولا مثل هذه القنابل المنطقية المغروسة. وبالإشارة إلى مقولة جون ميرشايمر حول الإرهاب،[3] يكفي إن اعتقد المهاجم المحتمل أن ترجيح فوزه بسرعة ليس جيداً بدرجة كافية؛ لأنه تم تعطيل نظمه.

قد يكون اللجوء إلى استراتيجية يحيط بها الغموض والشك في مصلحة الولايات المتحدة الأمريكية، وذلك بإقناع الدول الأخرى بالحرص الشديد على متابعة قوة تعتمد على الشبكات وتستخدم التقنيات العالية لمواجهة القدرات العسكرية الأمريكية، ومعنى

ذلك أنها يمكن أن تكون رادعة. ويعتمد الكثير على كيفية رد فعل الدول الأخرى تجاه اختراق قراصنة الإنترنت نظمها العسكرية وغرس طعوم داخلها، قابلة لتوليد رسائل شريرة عند تشغيلها؛ فتغير البيانات الاستشعارية، وتسبب انقطاعات في الشبكة، حتى إنها تسبب إخفاقاً في الأسلحة.[4] ومن الممكن الاستنتاج أنه إذا كانت الدولة المستهدَفة تعتقد أنها: (1) قد تم اختراقها، و(2) ليس لديها بديل عن النظم والمعدات الموجودة لديها، و(3) أن حصيلة الحرب وفق تقديرها ستكون أسوأ، و(4) أن لديها خياراً في ما إذا كانت ستمضي إلى الحرب، فسوف تتناقص رغبة الدولة في خوض الحرب.

كيف يمكن إثارة مثل هذا الشك والغموض؟ تتمثل أسرع الطرق المباشرة في اختراق مثل هذه النظم، ومن ثم توضيح أنه تم اختراقها. وليس من الضروري ادعاء المسؤولية؛ لأن الغرض ليس تأكيد قدرة الولايات المتحدة، وإنما الهدف إظهار ضعف النظم المستهدفة وانكشافها للهجمات عبر الإنترنت بطريقة تجعل أصحابها يشكُّون في نظمهم. أما إذا لم يكن الغرض هو تقديم برهان وإنما بث الغموض، فإن من غير الضروري جعل النتيجة واضحة سلفاً. والواقع أنه قد يكون من غير الحكمة أن يؤدي أول استعراض للقدرات إلى جعل تنفيذ الاستعراض الثاني أشد صعوبة، وبالتالي فقد يكون من المستحيل إثبات أن نظاماً ما كان، ويكون، وسيبقى عرضة للاختراق. لكن التلويح بالهجوم لا يترك أثراً محدداً، ومن ثم لا يستدعي أي إصلاح معين. وحتى إذا تمثل رد فعل أصحاب النظام على الإشاعات في إجراء إصلاحات عامة، مثل عملية فصل انتقائية أو تركيب حماية ضد البرامج الخبيثة، فلن يكون هناك ما يدل على أن هذه الإصلاحات العامة قد أعطت نتائج نافعة.

في بعض الحالات يمكن أن تكون الشائعة أقوى من الواقع. وعلى أي حال، يستغرق عدم العثور على شيء في غرفة، في المتوسط، ضعف الوقت الذي يستغرقه العثور على شيء فيها. والأسوأ من ذلك، إذا كان العثور على شيء حاسماً، والبحث وعدم العثور على شيء غيرَ حاسم، فإن إدراك المرء أنه لم يعثر على شيء يستغرق وقتاً أطول بكثير من الوقت الذي يستغرقه العثور على شيء. وقد يكون أصحاب النظم غير قادرين على الاطمئنان إلى أن

العثور على شيفرة يفترض أنها خبيثة سيحل المشكلة؛ لأنه لا يوجد دليل على أن ما تم العثور عليه هو الشيفرة الشريرة التي أشارت الشائعات إليها، ولعل مثل هذه الشيفرة هي عبارة عن خلل لا صلة له بأي طرف شرير، أو أنها وضعت هناك من قبل طرف ثالث.

إن قدراً كبيراً من المسألة يعتمد على ما يميل الآخرون لتصديقه حول قدرات الولايات المتحدة في التقنية بصورة عامة. ولا حاجة أبداً لأن يكشف محاربو الإنترنت الأمريكيون عن تقنيات هذه المناورات أو تلك، ولكن ينبغي التأكد من وجود تلميحات كافية تدل على أنهم يملكون المهارات المطلوبة. وقد يؤدي إخضاع ذلك الاعتقاد للاختبار إلى الإخفاق وإزالة السحر الذي سيطر عليهم. ومن المهم جداً معرفة أن هدف الهجوم ليس هو النظام نفسه، وإنما الثقة في ذلك النظام، وكذلك أي نظام يعتمد عليه الخصم.

إن ما يساعد هو القدرة على إقناع الآخرين بأنه ليس بإمكانهم حماية نظمهم حتى بعد الاهتمام المستمر بأمنهم. ولعلهم فحصوا وتأكدوا من كل شيء ثلاث مرات، ومع ذلك فإن محاربي الإنترنت يجدون طريقهم للدخول. ويُعتبر التأثير بالضرورة متوقعاً في المستقبل وليس متعلقاً بالماضي، فمن النادر حدوث هجوم على الأشخاص في هذه الأيام، فالهجوم هو الذي يصنع الخبر، ومع ذلك فليس هناك من فكرة جيدة عن الكيفية التي تم بها الهجوم أو على الأقل ما هي نقطة الضعف التي تم استغلالها لجعل الهجوم ممكناً.[5] ويبقى العديد من أدوات الهجوم على النظام المستهدف مزروعاً في ملفات سجله، أو حتى في البرمجيات الخبيثة نفسها. وحتى إذا كانت الجهات المستهدفة بالهجوم (مثل إيران) لا تستطيع معرفة ماذا تم فعله وكيف تم (مثل فيروس ستكسنت)، فقد يكون هناك آخرون يستطيعون ذلك (مثل، شركة بيلاروس، وبرنامج VirusBlokAda). إن عدد الهجمات البارزة التي تبقى أعمالها سراً غامضاً – ولا سيما طرق الاختراق والانتشار – يُعتبر عدداً صغيراً، وربما معدوماً. ومن الطبيعي أن أساليب هجوم معينة، وخاصة حرمان موزع من الخدمة، لا تحتوي على سر متوقع في المستقبل، فضلاً عن سر ماضٍ، في ما يتعلق بكيفية عملها؛ إذ تعتمد بشكل رئيسي على قوة عدوانية. أضف إلى ذلك أن أي شخص يتتبع الأخبار سيدرك وجود القرصنة في كل مكان. وليس من قبيل المبالغة افتراض أن أي

معلومات تمثل أهمية لدولة متطورة ولديها نظام مربوط بالإنترنت، قد تكون تسربت منذ وقت بعيد. وعند هذا المفصل يوجد العديد من نقاط الضعف في البرمجة عبر المواقع (مثل لغة جافا Java) وبرامج عرض الوثائق من أجل الإحساس بالأمان الشديد.

إن ضعف الدول الأقل تطوراً وانكشافها لإمكانية اقتحام آخرين لنظمها يتعزز وجوده عندما لا تفهم الجهة المستهدَفة بالفعل التقنية الكامنة خلف منظومات الأسلحة الخاصة بها. وعلى الرغم من إمكانية الاعتماد على الدول المتطورة في معرفة معداتها العسكرية بشكل أفضل من الدول غير المتطورة، فإن الفرق يكون عادة في الدرجة. فالدول المتطورة تحصل على مزيد من الفوائد من معداتها؛ فطائرة F-16 ستكون على الأرجح أكثر فاعلية في يدي طيار أمريكي مما هي في يدي طيار نمطي من العالم الثالث. كذلك تقوم المؤسسات العسكرية المتقدمة أيضاً بصيانة معداتها بصورة أفضل، ومع ذلك فإن طائرة F-16 تُعتبر آلة حرب، حتى إذا كان يقودها طيار أقل خبرة وتلقى صيانة قليلة الخبرة.

مع هذا، قد يكون نظام المعلومات عديم القيمة في أيدي مستخدمين غير متطورين أو غير مهتمين بالأمن. فالنظم التي لا تحظى بدفاع قوي يمكن أن تتعرض، تحت الضغط، إلى تسرب المعلومات، أو تنهار بشكل مفاجئ، أو تزود المقاتلين وغيرهم من صناع القرار بمعلومات سيئة. ومن الممكن في الحرب عبر الإنترنت أن يكون ثمة قرصان كبير أكثر فاعلية تقريباً من قرصان جيد بطرق لا تميز الفرق بين مصلح كبير للأجهزة ومصلح جيد لها. ولعل الصعوبة التي تواجه بعض الدول الأقل تقدماً في الحصول على قدرات هجومية عبر الإنترنت راجعة إلى ضعف المرافق التعليمية وافتقار الكوادر إلى التعليم المناسب. ومع ذلك، فإن عدم إمكانية حصولها على الشيفرة الخاصة بمصدر أجهزتها، أو عدم إنشائها شيفرة خاصة بها، وكذلك قلة عدد من أنشأوا لديها شيفرة تشغيلية خاصة بهم، كل ذلك يجعل نظمها العسكرية عرضة للهجوم عبر الإنترنت أكثر من النظم المماثلة الأخرى في الدول المتطورة. كما أن دول العالم الثالث التي تمتلك نظماً جاهزة، لعلها تستخدم أيضاً تصاميم وإجراءات تشغيل قياسية، الأمر الذي يزيد من توقعات تعرّضها لهجمات أكثر مما

هو متوقع بالنسبة إلى الدول التي تفهم نظمها بدرجة جيدة تكفي لضبطها بما يتناسب مع ظروفها الفريدة الخاصة بها. وما لم تكن تلك الدول خاضعة لعقوبات أمريكية رسمية، فإن نظمها على الأغلب سيتم صيانتها بواسطة شركات أمريكية. وإذا كانت الحوسبة السحابية* بمستوى حماس مورديها، فقد يتم تخزين مكونات حساسة لنظم التحكم الوطنية لدى دول أخرى، ويتم تشغيلها من قبل هيئات أخرى يبدو أن الشركات الأمريكية هي المضيفة الأكثر احتمالاً لها.

هل ستنجح مثل هذه الاستراتيجية مع روسيا والصين؟

بالنسبة إلى روسيا يكاد الجواب يكون "لا". أولاً، تُعتبر القدرات الروسية في الحرب عبر الإنترنت متقدمة جداً، وتتلاءم مع دولة مكرَّسة للتمويه في الحرب، وتنعم بعدد وافر من علماء الرياضيات من الطراز العالمي.[6] قد يخشى الروس القدرات الأمريكية، ولاسيما في الإلكترونيات، ولكن من غير المرجح اعتبارهم مرتبكين على نحو خاص (وبخاصة إذا لم تكن الإلكترونيات جزءاً من رزمة الحرب عبر الإنترنت). ثانياً، إن الورقة العسكرية القوية في يد الروس ليست دمج النظم المعقدة للإلكترونيات والشبكات. ولأنهم يفتقرون إلى الثقة بقواتهم المسلحة التقليدية، فإنهم يعتمدون بشدة على ترسانتهم النووية. ولهذا فمن المستبعد أن يتم تحويل استراتيجتهم الاستثمارية بسبب تطوير الولايات المتحدة أسلحة الفضاء الإلكتروني.

أما في حالة الصين، فلعل الإجابة مختلفة. فمن المؤكد أن الصين أبدت حماساً للحرب عبر الإنترنت، ويظهر ذلك من عقيدتها، ومن الحجم الكبير لعمليات الاختراق التي ينسبها الناس إليها. وتتجه المواهب الصينية في الفضاء الإلكتروني نحو الكم، وبما يتلاءم مع التركيز على التجسس عبر الإنترنت، أكثر من اتجاهها نحو نوع الجودة المطلوبة

* الحوسبة السحابية أو السحابة الإلكترونية cloud computing، هي نوع من الحوسبة التي تعتمد على تقاسم المصادر بدلاً من الاعتماد على الخوادم المحلية أو الأجهزة الشخصية للتعامل مع التطبيقات. وكلمة السحابة cloud في هذا المجال هي رمز يشير إلى شبكة الإنترنت؛ وبهذا فهي تعني الحوسبة المعتمدة على الإنترنت، حيث الخدمات المختلفة مثل الخوادم ومستودعات التخزين والتطبيقات تصل إلى أجهزة المنظمات والشركات من خلال الشبكة. (المحرر)

لاختراق النظم العسكرية المحصنة. أضف إلى ذلك أن استراتيجية الاستثمار العسكري الصينية تختلف تماماً عن استراتيجية روسيا. فالصينيون أقل اهتماماً بتحقيق التكافؤ النووي، وأكثر اهتماماً بمتابعة استراتيجيات مقاومة الدخول أو النفاذ إلى الشبكات، وتعتمد تلك المقاومة على أجهزة الاستشعار والمراقبة والصواريخ، ما يتطلب مستويات عليا من تكامل النظم، ومن ثم التشبيك.[7] وتترك هذه العوامل بعض المجال أمام موقف الردع الأمريكي القائم على قدرات الحرب عبر الإنترنت ضد الصين.

كيف يمكن أن يؤثر الخوف من الاختراق في السلوك العملياتي للعدو؟

ينطوي أحد أهداف إظهار قدرات الحرب عبر الإنترنت على إجبار الدول على أن تأخذ في الحسبان إمكانية تعطل النظام والارتباك الناجم عن ذلك، ومن ثم كبح حماسها للحرب. ولكن هل سيتحقق هذا الهدف؟ ربما لا. أولاً، عندما يتعلق الأمر بالحرب، فإن جميع المدافعين تقريباً، ونسبة مذهلة من المهاجمين، يعتقدون أنه قد تم وضعهم في موقف لا خيار لهم فيه سوى خوض الحرب؛ لأن البديل سيكون أسوأ، وهذا ما اعتقده اليابانيون عام 1941 أو الألمان عام 1914، فقد أخفق الخوف في ردعهم. ثانياً، ما مدى حاجة الدول التي تفكر بمثل هذه الأعمال إلى نظم عالية التقنية لكي تحقق النجاح؟ تدعو الحاجة إلى عدد كبير من النظم ذات التقنية العالية (مثل الحرب الإلكترونية) لاستخدامها ضد الخصوم المماثلين في التطور، وليس رجال العصابات. فالتهديد الذي يبدو كبيراً في وقت السلم (عندما تكون النظم منكشفة بحكم كونها موصولة بالإنترنت) يمكن أن يبدو أصغر في وقت الحرب (عندما تكون النظم مصممة للصمود والبقاء، ويعود ذلك في جانب منه إلى كونها مفصولة عن العالم الخارجي). أخيراً، ببساطة قد لا تؤمن الجهة المستهدفة بأن قدرات الولايات المتحدة في الحرب عبر الإنترنت جيدة بدرجة كافية لإحباط معنويات القوات العسكرية تماماً، ليس في أوقات السلم، وبالتأكيد ليس عندما تقرع طبول الحرب، فخوض الحرب يتطلب التغلب على العديد من المخاوف؛ وقد يكون الخوف من الاختراق مجرد مصدر خوف آخر.

إن إقناع أطراف أخرى أن هناك عفريتاً جاهزاً للانطلاق في نظمهم يحمل في طياته مخاطر أخرى. ففي الحد الأدنى، إذا حافظوا على رباطة الجأش فإنهم على الأرجح سيولون مزيداً من الانتباه لأمن العمليات بعد التلويح بقدرات الهجوم عبر الإنترنت الأمريكية، وأي اعتقاد بأن القوة الموجهة الموجودة في نظمهم هي جاسوس سيدفعهم إلى ممارسة مزيد من أمن الموظفين. وإذا تحولت رياح التحالف وتعيّن على الولايات المتحدة القتال إلى جانب هذه الدول، فإن تلميحات بالاختراق يمكن أن تجعل من الصعب على الولايات المتحدة الأمريكية العمل مع الشركاء الجدد. وقد تصبح العلاقات الحميدة سابقاً مع بلد مستهدف أشد صعوبة إن شك "الشريك" بأن التفاعل مع القوات الأمريكية يكشف كيف يتم تشغيل نظمه وتشبيكها، ومن ثم، أين يمكن للولايات المتحدة زرع برامج خبيثة بحيث تحقق أفضل النتائج، وكيف.

بمجرد أن تشعر دول أخرى بأن الولايات المتحدة تكمن وراء مخاوفهم، فقد يكون الواقع أمراً ثانوياً. وقد تكون الدول التي تتيقن أن قواتها المسلحة قد تعرضت لهجوم أقل ميلاً لتوجيه اللوم لجيرانها الذين لا يتمتعون بدرجة من التطور تكفي لشن مثل هذا الهجوم. وبهذا، ستكون تلك الدولة أكثر ميلاً لتوجيه اللوم إلى دولة متقدمة تقنياً مثل الولايات المتحدة الأمريكية أو إسرائيل. وبالفعل، فإن انتشار قدرات الهجوم عبر الإنترنت يجعل من السهل على تلك الدول أن تعتبر الولايات المتحدة مسؤولة عن أي عطل في المعدات العسكرية، وحتى عن أية حوادث أو أخطاء بشرية؛ فغريزة لوم الآخرين تسبق في وجودها الفضاء الإلكتروني؛ فقد أقنعت مصر نفسها، لبضعة أيام في يونيو 1967، بأنه لم يكن الإسرائيليون يستطيعون تدمير قواتها الجوية، ومن ثم، فلا بد أن الأمريكيين هم من فعلوا ذلك. إن المؤسسات العسكرية التي تستطيع إعفاء نفسها من المسؤولية أمام الشعب باستخدام مثل هذا العذر، يمكنها وقاية نفسها من عواقب أخطائها، كما يمكنها أن تحافظ على نفوذها وسلطتها فترة أطول مما ينبغي لها. وكبديل لذلك، فإنه بقدر ما يقنع هؤلاء القادة أنفسهم بأعذارهم، فإنهم يمكن أن يخفقوا في التعلم من أخطائهم، وهذا في الواقع مفيد للولايات المتحدة الأمريكية.

قد تستنتج المؤسسات العسكرية المستهدفة أيضاً أن الاعتماد على مصادر أجنبية لأجهزة المعالجة المنطقية يُعدُّ خطيراً، ويمكن أن يحفزها ذلك إلى بناء قدرات إنتاجية محلية، أو- بدلاً من ذلك - الضغط على مورديهم لتسليمهم شيفرة مصدر النظم. ويمكن أن يكون كلا الأمرين سلبياً بالنسبة إلى الولايات المتحدة ما دامت شركات أمريكية هي التي تقوم بتوريد هذه الأجهزة. ولعل الشكوك نفسها تؤثر في أجندة الجهة المستهدفة نحو الأجهزة المدنية، مثل الموجهات (الراوترات) المستخدمة في شبكاتها. وكرد على ذلك، قد يلجؤون إلى التوطين؛ أي الاعتماد على الداخل، وإلى شيفرة مصدر أكثر شفافية، وتدريب أفضل على الدفاع عبر الإنترنت، فإذا أقنعوا أنفسهم بأن الالتزام بمعيار ويندوز/ إنتل Windows/Intel هو أصل القدرة الأمريكية على اختراق أجهزتهم، فقد يميلون نحو نظم تشغيل أكثر انفتاحاً أو التعاون مع دول أخرى، مثل الصين، تسعى لبناء طبقة أساسية من المكونات وشيفرة من المعتقد أنها لن تتم السيطرة عليها من قبل الشركات الأمريكية.[8]

لن تختفي المشكلة إذا تبيَّن أن التلميحات إلى أنه تم اختراق نظم أخرى غير صحيحة. افترض أن الولايات المتحدة الأمريكية أقنعت الآخرين بأن بإمكانها اعتراض الأجهزة العسكرية لأي جهة، ثم اندلعت حرب ولم تُصَبْ أي أجهزة بالخلل بطريقة لا تفسير لها، فسوف يستنتج المحللون أن الولايات المتحدة اختارت ألا تعطل النظم المتطورة لأحد الطرفين. إذا كانت أجهزة أحد الطرفين تعمل، قد يفترض الآخرون أن هذا برهان على أنه لا بد أن الولايات المتحدة قد انحازت، بل ويعتبرونها مسؤولة عن الفظائع المرتبطة بمثل هذه المعدات العسكرية. وقد لا يعيرون الحجج المقابلة اهتماماً: بأن الولايات المتحدة لمحت إلى أنه "قد يكون" وليس "سيكون"، فهي لا يمكنها أن تدخل إلى معدات الجميع؛ فبعض المعدات لا يمكن الوصول إليه من الخارج، ومعدات أخرى - مثل الكلاشنكوف AK-47 - لا تحوي أي إلكترونيات يمكن النفاذ إليها. وقبل انتشار التلميحات، لم يكن أحد ليتخيل أنه يمكن تعطيل المعدات العسكرية عن بعد، ولكن بعد ذلك لم يستطع أحد أن يتصور أن الولايات المتحدة غير قادرة على فعل ذلك.

كيف يمكن أن تؤثر مخاوف الاختراق في الاستثمارات الدفاعية؟

يمكن أن تتّبع دولة تخشى الاختراق استراتيجيات تعويضية، فقد تلاحظ أن آثار الهجمات عبر الإنترنت مؤقتة ومن الصعب تكرارها، ثم تحافظ على استراتيجيتها في الاستثمارات الدفاعية بعد إقناع نفسها بأنها - حتى إذا لم تنجح أسلحتها عند استخدامها لأول مرة - يمكن أن تجتاز المناوشات الأولية وتستعيد فاعليتها لجولات الصراع الأخرى لاحقاً. ومن شأن مثل هذا المنظور أن يُغفل قدرة المؤسسات العسكرية ذات التقنية العالية على إنهاء حملات تقليدية ناجحة في غضون أيام، وليس شهور أو أعوام. ولعل صاحب النظام المتطور يكون قادراً على الكشف عن نقطة ضعف مستغلة حديثاً في غضون ساعات ويصلحها خلال ساعات أو أيام بعد اكتشافها، ولاسيما إذا كان ذلك بعون خارجي. ولكن هل يستطيع صاحب نظام غير متطور، وهو على خلاف مع العالم المتطور ويواجه هجوماً أمريكياً متطوراً عبر الإنترنت، أن يعلق آماله على التعافي بمثل هذه السرعة؟ قد تدرك الدولة أيضاً أنه بعد إصابة نظام بالخلل، فربما لا يراهن المحاربون عليه إلا بعد علاجه بشكل تام ومثبت، وهذه عملية تستغرق زمناً أطول من مجرد زوال الأعراض.

إذا توقعت دولٌ إمكانية اختراق نظمها المربوطة بالشبكة، فقد تتخلى عن حرب مرتبطة بالشبكات. ما الذي يجعلها تسعى لمواجهة أعداء بأسلحة يمكن أن تخفق إخفاقاً محقَّقاً عند استخدامها؟ وبالمقابل، بالنسبة إلى الولايات المتحدة، إذا كانت تستطيع فعلاً التغلب على قدرات الطرف الآخر العسكرية التي تعتمد على الشبكات، فلماذا تريد صرفهم عن بنائها والاعتماد عليها؟ لعل أحد الأسباب يكمن في أن الولايات المتحدة لا يمكنها التيقن من قدرتها على دحر مثل هذه القدرات، ولكنها تريد أن تقنع الآخرين بأنها تستطيع. ولعل هناك سبباً آخر هو أنها تريد ردع الآخرين عن بناء قدرات عسكرية؛ لأن ذلك من شأنه أن يقود إلى سياسة أمنية أكثر هجومية، تؤدي بالتالي إلى البدء في صراع أو مواصلته، في الوقت الذي تتحقق فيه مصلحة أمن الولايات المتحدة

الأمريكية بعدم استخدامهم مثل هـذه القـدرات، أكثـر مـن تحققهـا بـدحرهم بعـد أن يستخدموها. لكن إذا رأت الولايات المتحدة أن الطرف الآخر سيمضي قُدُماً مهما يكن، فقد يكون من الأفضل السكوت بشأن ثقتها بقدرتها على دحر تلك القدرات.

لعل استراتيجية رد الجهة المستهدَفة تكمن في الاعتماد على أسلحة أقـل تقنيـة بحيـث تكون صامدة ضد الهجوم عبر الإنترنت؛ لأنها ليـست مـشبوكة بـأي شيء. لـذا، إذا تخـلى خصوم الولايات المتحدة عن التشبيك، فهل تُهزم استراتيجية الغموض والشك بـذلك أم ستنتصر؟ هل سيُسهم النجاح في صرف الخصم المحتمل عـن التحـدي المتمثـل في التقنيـة العالية، في تحقيق أفضل المصالح للولايات المتحدة الأمريكية؟ إن الكثير يعتمد عـلى نـوع الحروب التي تشعر الولايات المتحدة بالقلق حيالها. فـإذا كـان الهـدف هـو أن تجعـل مـن الصعب جداً استخدام الأسلحة التقليدية لمقاومة الغزو أو الإكراه (وليس لمحاربة تمـرّد)، فإن القوات ذات التقنية المنخفضة لا تُعتـبر نـداً للولايـات المتحـدة. فالتـضحية بـالجودة النوعية تزوّد الآخرين بالوسـيلة للـسعي وراء الكـم، ولكـن حتـى الآن لم يكـن التـوازن بالنسبة للآخرين جيداً بشكل خاص، فالجودة النوعية تنتصر دائماً.

ثمة استراتيجية مضادة أكثر دقة تتمثل في تشبيك آلات القتال الحربيـة بحيـث تبقـى مفصولة عن الشبكة والأشخاص. وتتصف هذه الاستراتيجية بمزايا السماح بـالعزل عـن الشبكات وعن الإنترنت كاستراتيجية دفاعية، وتفادي بعض نقاط الـضعف الناشـئة مـن الأخطاء البشرية (ولاسيما الأخطاء المتصلة بالتحقق، مثل كلمات المرور والرموز). إذا تـم الإفراط في بيع محترفي الشبكات المقاتلين، فإن الدول التي تُمـسك عـن شرائهـم ستحـسن صنعاً مع نفسها، أو يمكنها أن تشبك معداتها في ما بينها، ولكنها تفصلها عن بقيـة العـالم. ولعل حرمان الذات من الخدمة، يقلـل مـن قـدرة المؤسـسة العـسكرية عـلى الـتعلم مـن الآخرين، ومن نفسها إلى حد ما. ومـع ذلـك فهنـاك العديـد مـن المؤسـسات العـسكرية المنطوية على نفسها أو المعزولة، والتي - حتى في حال عدم وجود حرب عـبر الإنترنـت - تميل إلى أن تقلل من خبرات الآخرين التي يمكن أن تتعلم شيئاً منها.

علم جبر التخويف المباشر

إذا أخفق الإعلان عن القدرات الهجومية في ردع الهجوم، فهل يمكن للاستعراض أن يوفر قدرة على القسر والإكراه؟[9] يكمن أحد المآزق في مدى الاعتراف بالاستعراض. خذ في الاعتبار علم الجبر. افترض أنه إن قام مهاجم، ولنسمها الحالة "ع"، بالكشف عن نفسه دون غموض من خلال الهجوم عبر الإنترنت، فإنه يخسر بسبب انتقام الخصم أكثر مما يكسب من الإكراه. فإذا أخفى نفسه تماماً فإنه لا يحصد أي فائدة من الإكراه (فالضرر يمكن بسهولة أن يكون قد حدث صدفة). ويبدو أن مستويات الضمان المتوسطة تؤدي إلى أمور سلبية محضة ومباشرة؛ فعلى سبيل المثال، إذا كانت الجهة المستهدَفة تظن أن احتمال أن يكون المهاجم هو "ع" بنسبة 50:50، فإن فوائد الإكراه تكون نصف ما لو كانت الجهة المستهدفة على يقين.[10] بالمثل، فإن نسبة احتمال الانتقام – وبالتالي التكلفة المتوقعة لتحمل مثل هذا الانتقام – هي نصف ما ستكون عليه لو أن الجهة المستهدفة كانت متيقنة. وهكذا، نجد من وجهة نظر "ع" أن فوائد الإكراه وكذلك التكلفة المتوقعة للانتقام قد انتصفت أو تساوت. ولكن هذا يترك الأمر سلبياً محضاً، وبالتالي يبدو أنه لا يمكن أن يفوز.

ولكن هل نسبة احتمال الانتقام في الواقع هي نفسها كنسبة الاحتمال المتصورة بأن "ع" هو المهاجم؟ وبعبارات أكثر تحديداً، هل نسبة احتمال الانتقام هي افتراض 50:50 إذا كانت الجهة المستهدَفة تظن أن احتمال أن يكون "ع" هو المهاجم بنسبة 50:50؟ يعتمد الأمر بشكل كبير على مدى نفور الجهة المستهدفة من المخاطرة. إذا كانت الجهة المستهدفة تخشى عواقب عدم الانتقام من المهاجم الحقيقي (عامل الضعف) أكثر من خشيتها عواقب الانتقام من دولة بريئة (عامل الخطأ)، فإنها لا تحتاج إلى ثقة كبيرة في عزوها الهجوم إلى أحد ما لإقناع نفسها بالرد. والذي يبدو أكثر احتمالاً هو أن الجهة المستهدفة تخشى عامل الخطأ أكثر من خشيتها عامل الضعف، ولن يكون مستوى الثقة 50:50 كافياً لإقناعها بالانتقام. وفي تلك الحالة، فإن احتمال أن تنتقم الجهة المستهدفة عندما تكون نصف متيقنة من أن "ع" هو من فعلها أقل من 50:50.[11]

إذا كان الأمر كذلك، فإن قوة الهجوم عبر الإنترنت عندما تظن الجهة المستهدَفة أن "ع" قد نفذه – ومن ثم فائدة الإكراه للحالة "ع" – يمكن أن تكون أكبر من تكلفة الانتقام المتوقعة. ومع هذا، فإن تكلفة الانتقام وحدها ينبغي أخذها في الاعتبار عندما يكون عزو الهجوم إلى أحد ما واضحاً تماماً، بحيث تعتقد الجهة المستهدفة أن نسبة احتمال ارتكاب خطأ منخفضة بدرجة كافية.

إن الدرس الأكبر هو أن الهجوم الذي يمكن نسبته إلى المهاجم، قد يكون مفيداً للمهاجم، أكثر من الهجوم الذي لا يُنسب إلى أحد حتى لو كان الأخير أشد وضوحاً. ومن جانبها، قد تبذل الجهة المستهدفة قصارى جهدها للمبالغة في احتمال الانتقام، وهذا هو الأفضل لإجهاض حسابات المهاجم. لكن بالنظر إلى طبيعة الأزمات وحالات الغموض الطبيعية في الفضاء الإلكتروني، فمن المرجح أن يتعامل المهاجم بالفعل مع قدر كبير من المعلومات الغامضة.

إذا كانت أهداف المهاجم الإكراهية أكبر، ولا تتوقف على من تظن الجهة المستهدفة أنه المهاجم، فإن كسبه الصافي سيكون أكبر. إن قولك لشخص آخر: "افعل ما أريد أنا"، دون تحديد من "أنا"، هو أمر صعب، ولكنه ليس بالمستحيل. افرض أن بلداً (مثلاً، دولة إسلامية) تحالفت في مصالحها مع مجتمع أكبر (مثلاً، الأمة الإسلامية)، ولاسيما مجتمع فيه جهات فاعلة وقوية ليست دولاً. وإذا كان الأمر كذلك، فمن الممكن إقامة بعض الارتباط بين توقيت الهجوم وطبيعته (مثلاً، في أعقاب عمل عسكري ضد أفراد مسلمين) وبين السلوك المطلوب من الجهة التي استهدفها الهجوم (مثلاً، التوقف عن مهاجمة الإسلام) دون توجيه اتهام بالضرورة للدولة المهاجمة. فالدولة المتهمة بشن هجوم عبر الإنترنت يمكن أن ترد على التهمة بأن لها أصدقاء لا يمكنها السيطرة عليهم، ولكن لهم غضبة ينبغي الاعتراف بها. إن ما يسمى القراصنة الوطنيين قد يكونون مواطنين في دولة متهمة من دون أن تبدو تلك الدولة منافقة مادامت تقوم بمسعى ذي مصداقية لإخضاعهم للسيطرة الحقيقية. وبدلاً من ذلك، يمكن للدولة أن تشعر بالرضى والارتياح لهجمات الإنترنت التي تعاقب السلوك الذي يتنافى ومصالح المجتمع.

وفي الوقت نفسه، لا توجد ضرورة للإقرار بدعم تلك الهجمات أو حمايتها أو حتى رعايتها. إن الإمكانات الإكراهية للمهاجم قد تكون محصورة في القيم التي يؤمن بها المجتمع؛ وهي عادةً واحدة من بين مصالحها العامة (فمثلاً، إن ما يمكن أن يكون جيداً لاتخاذ إجراء ضد عدو مشترك، قد لا يكون جيداً لتأكيد مصالح خاصة، مثل حقوق المياه). ولكن ذلك قد يكون كافياً.

تُرى، هل سيتطور سلوك الدولة المستهدفة في الاتجاه الذي يرغب فيه المهاجم نتيجةً للإكراه (سؤال يتلاءم والتهديدات الناشطة)؟ افترض أمرين: أولاً، أن الهجمات التي تؤدي إلى ألمٍ أقل من عتبة الحساسية sensitivity threshold، تُعدُّ أضعف من أن تجبر الدولة المستهدفة. ثانياً، إن الهجمات التي تسفر عن ألمٍ أكبر من عتبة الاستجابة response threshold تدفع الدولة المستهدفة إلى الرد، أو على الأقل تصبح أقل تعاوناً (بصورة إجمالية على الأقل، إن لم يكن بالضرورة في النقطة المعنية). وإذا كانت عتبة الحساسية أقل من عتبة الاستجابة، فقد تكون ثمة منطقة بينهما، حيث تذعن الدولة المستهدفة فيها لإرادة المهاجم. ولكن إذا كان الطرفان على النقيض من ذلك، فلن يؤدي أي هجوم، مهما تمت حساباته بعناية، إلى تغيير سياسة الدولة المستهدفة إلى الاتجاه المطلوب. فإما أن يكون الهجوم أضعف من أن يؤدي إلى الإكراه بدرجة كافية، أو أقوى من أن يتم امتصاصه من دون ردّ، وربما كلا الأمرين. فقد أثبتت الولايات المتحدة مرتين على الأقل، وبشكل لافت، أنها ترد بقسوة إذا وقع هجوم عليها، كما حدث مع عمليات بيرل هاربر وهجمات الحادي عشر من سبتمبر، على حد سواء.[12]

إذا سلّمنا بذلك، فقد لا يكون الأول عملاً إكراهياً (لأن اليابان كانت تعتقد أنه سيحدث قتال بينها وبين الولايات المتحدة الأمريكية في كل الأحوال، سواء عاجلاً أو آجلاً)، ولعل الثاني تم تنفيذه لدفع الولايات المتحدة إلى التدخل في أفغانستان. ومع ذلك، فإننا إذا وضعنا مثل هذه الفروق جانباً، وجدنا أن الولايات المتحدة أثبتت أن إكراهها قد لا يكون مفيداً بصورة خاصة عندما تكون عتبة الاستجابة للجهة المستهدفة أخفض من عتبة حساسيتها. ثمة قدر كبير من الأدبيات حول موضوع الإكراه، توضح

مدى صعوبة إكراه الدول على الإذعان للمطالب، حتى بأسلحة الطاقة الحركية*.[13] ومن الصعب إثبات أن أسلحة الفضاء الإلكتروني - بكل غموضها - ستقوم بعمل أفضل.

ويمكن للمهاجم أن يقود حملة قسر سرية باستخدام هجمات سرية، بمعنى أنه يمكن أن يستهدف أنظمة من شأن إخفاقها أو فسادها أن يحمِّل الحكومة المستهدفة تكاليف باهظة، ولكن تأثيرات ذلك لا تكون واضحة للجمهور. ومن خلال القيام بذلك، يغامر المهاجم بأن تكون مراكز حساسية صانعي السياسات وعتبات استجابتهم مختلفة عما هي عليه لدى الجمهور العام. فصانعو السياسات المتألمون وغير المقيدين بالرأي العام قد يكونون أسهل استجابة للقسر، وخصوصاً إذا كانت الاستجابة للقسر غير بادية للجمهور.

لعل التخويف المباشر أكثر فاعلية إذا تم تنظيم الهجوم عبر الإنترنت بشكل واضح لإيقاع أضرار أقل كثيراً مما يمكن أن يحدث.[14] إن جميع مساعي الإكراه تثير لدى الضحية مزيجاً من الغضب بسبب التعرض للضربة والخوف من الضربة الثانية. فإذا كانت الضربة الأولى خفيفة، فمن المحتمل تهدئة الغضب؛ إذ رغم وضوح الإهانة فإن الأضرار ليست كذلك. ومع ذلك، فإن عنصر الخوف يُعدُّ كبيراً في حالتي الضربة التي يتم التلويح بها والضربة التي يتم توجيهها فعلاً، مادامت الجهة المستهدفة تدرك - في الواقع - أن الضربة قد تم التلويح بها (مع العلم بأن غموض الفضاء الإلكتروني يمكن أن يضيّع وضوح الرسالة).

تناقضات التخويف

هل تُعتبر المكاسب القصيرة الأمد من هذا النوع من التخويف، حتى إذا كان كامناً، جديرة بالإزعاج الطويل الأمد المتمثل في الإسراع بتطوير طراز معين من الأسلحة؟ في سباق التسلح النووي بين الولايات المتحدة الأمريكية والاتحاد السوفيتي كان نيكيتا

* أسلحة الطاقة الحركية kinetic weapons؛ هي التي تستمد قوتها التدميرية من الطاقة الحركية للمقذوفات التي ترتطم بأهدافها بسرعات عالية. (المترجم)

خروشوف يتباهى بأن بلاده استطاعت إنتاج الصواريخ "مثل النقانق". وردّت الولايات المتحدة بالتعجيل ببرنامجها الصاروخي. وبحلول عام 1961، قبل عام من أزمة الصواريخ الكوبية، علمت الولايات المتحدة أنها تتمتع بتفوق استراتيجي في نظم الإطلاق النووية، ولاسيما الصواريخ. وكذلك السوفييت، فقد أقنعتهم تصورات مماثلة بشحن صواريخ إلى كوبا لتعديل التوازن الاستراتيجي. وتمثل رد الفعل السوفيتي - عندما اضطر السوفييت إلى التراجع في كوبا - في التعجيل ببرامجهم لتحقيق التكافؤ، وقد تحقق لهم ذلك. وبذلك هيأوا الأجواء لمحادثات الحد من الأسلحة الاستراتيجية. وربما لو لم يتباهَ أي من الطرفين بقدراته لأمكن أن يتحقق التكافؤ والمفاوضات، وفي الوقت نفسه تقريباً، ولكن بمستويات أقل كثيراً. ولا يكاد السباق الصاروخي يمثل حالة منفردة، فقد سبق أن حدث ذلك في حالة التنافس الأنجلو-ألماني في بناء السفن قبل الحرب العالمية الأولى.

مع ذلك، لا يُعتبر سباق التسلح عبر الإنترنت المسار الأكثر ترجيحاً للأحداث. وفي تباين كبير مع معظم الأسلحة العسكرية، من شأن الأضرار الناجمة عن هجوم عبر الإنترنت أن تعكس خصائص الجهة المستهدفة أكثر مما تعكس خصائص السلاح. وبالتالي فإن التنافس للحد من نقاط الضعف قد يلقي بظلاله على التنافس لاكتشاف هذه النقاط واستغلالها. وحتى إن لم يكن الأمر كذلك، فإن قدرات أسلحة الإنترنت موضع خلاف خطير لدى الطرفين، وهذه الملاحظة هي أساس هذه المناقشة كلها. أما الأعداد التي تفيد بتوازن الصواريخ أو البوارج الحربية (بوارج حقبة الحرب العالمية الأولى)، فليس لها مكافِئات ذات مغزى في الفضاء الإلكتروني.

السياسة الأمريكية وشرعنة الحرب عبر الإنترنت

يتصف الموقف الأمريكي الحالي من أسلحة الفضاء الإلكتروني بالخجل، فهو يقع بين الموقف الأمريكي من الأسلحة النووية (رهيبة، غير أنها مفيدة لمناسبات خاصة جداً) والأسلحة الكيماوية والبيولوجية (أمر بالغ الإثم حتى التفكير فيه). وعلى الرغم من أنه لا توجد سياسة رسمية تؤكد أن الولايات المتحدة ستستخدم الهجمات عبر الإنترنت، فإنه لم

يكن ثمة تفنيد جاد للافتراض القائل بأن الولايات المتحدة كانت مسؤولة عن هجمات ستكسنت.[15] كما نقلت الصحافة تقارير – دون تفنيد أيضاً – تفيد بأن وكالة مشروعات الأبحاث الدفاعية المتقدمة Defense Advanced Research Projects Agency كانت تعمل على تطوير قدرات حربية هجومية عبر الإنترنت.[16] وقد أعلنت المملكة المتحدة وكندا عن رغبات مماثلة.[17]

لا تمضي دول أخرى، كالصين مثلاً، إلى ذلك الحد من حيث الاعتراف بقدراتها الهجومية عبر الإنترنت والأسباب التي يمكن أن تدعوها إلى استخدامها. ومع هذا، فإن إنكارها للتشويش لا يُنظر إليه بمصداقية. وما هذا إلا انعكاس جزئي للآراء الواسعة التي تتجادل بشأن ما إذا كانت قدرات الهجوم عبر الإنترنت تُعتبر أسلحة إرباك وتعطيل. فقد أثبتت الهجمات على إستونيا أنها ما هي إلا أسلحة إزعاج شامل. وتتم معاملة الهجمات عبر الإنترنت على أساس يومي كقضايا جنائية، الأمر الذي ينزع الشرعية عنها كأدوات للحكم وإدارة الدولة. ومن غير الواضح إذا ما كان نزع الشرعية هذا مرتبطاً بالعمل في حد ذاته أو باستخدامه من قبل أطراف خاصة. إن الولايات المتحدة الأمريكية تفضل أن تعامل الدول الأخرى جرائم الإنترنت بمزيد من الجدية وتتجنب الإغراء بخصخصة استخدام القوة العسكرية في الفضاء الإلكتروني (مثل، الروابط بين الحكومة الروسية وشبكة الأعمال الروسية، أو بين الصين وقراصنتها المستقلين و"الوطنيين"). ومن المفارقات أن التحركات نحو شرعنة مثل هذه الأسلحة، يمكن أن تجعل من الأسهل على الدول الأخرى أن تأخذ الملكية، ومن ثم، تتحمل المسؤولية عن استخدام شعوبها لمثل هذه الأسلحة.

وبعد هذا كله، فلعل الحرب عبر الإنترنت قد عبرت بالفعل عتبة اكتساب الشرعية، وقد يكون تحقق لها ذلك، ضد الأهداف العسكرية على الأقل، منذ عام 1999. [18] وتقوم الولايات المتحدة الأمريكية والدول التي تملك قدرات مثلها ببحث الجهود الرامية لنزع الشرعية عن استخدام الحرب عبر الإنترنت ضد أصناف معينة من الأهداف (مثل، المستشفيات). وقد ينتج عن ذلك توافق عالمي أو حتى معاهدة. وإذا كان الأمر كذلك، فإن التلويح بالقدرة على تخطي هذه المعايير سيكون مثار إشكاليات.

التلويح بالهجوم عبر الإنترنت في مواجهة نووية

ليس من السهل التصدي للدول التي تهدد باستخدام قدراتها النووية إذا لم تتماشَ الولايات المتحدة الأمريكية مع رغباتها. هل من الممكن أن يؤثر التلويح بقدرات الهجوم عبر الإنترنت في مضمار مثل هذه المواجهات؟ وقد يسهم استقصاء آليات مثل هذا التأثير في إلقاء مزيد من الضوء على الفرص والقيود للتلويح بقدرات الهجوم عبر الإنترنت (حتى إن لم تكن بالضرورة تسهم في توسيع فهمنا للمواجهات النووية بهذه الصورة).

وبذلك، فإننا لن ندَّعي بالضرورة أن قدرات الهجوم الأمريكية عبر الإنترنت يمكن بشكل موثوق به أن تتغلب على القدرات النووية للأعداء. فالدول، في المحصلة، تولي نظم أسلحتها النووية قدراً كبيراً من الاهتمام من أجل اليوم الذي يعتمد فيه بقاء نظامها على جاهزية أسلحتها للاستخدام. فالدول النووية تمضي بعيداً في سبيل حماية قيادتها وسيطرتها على هذه الأسلحة. فقد جاءت الأسلحة النووية والصواريخ الضخمة التي تحملها قبل وقت طويل من الثورة الرقمية، وتبقى الأسلحة تناظرية analog إلى حد بعيد، على الرغم من التطوير اللاحق للقيادة والسيطرة وتوجيه الصواريخ الدقيق، وهذه تحتوي بالطبع على عناصر رقمية.

لكن لا يمكن بسهولة دحض إمكانية اختراق الولايات المتحدة نظم القيادة والسيطرة أو عمليات النظم النووية. ومما لا ريب فيه أن قادة إيران ظنوا أن عزل منشأة نتانز التي تتضمن أجهزة الطرد المركزي، جعلها آمنة من الهجوم عبر الإنترنت، ثم عرفوا بستكسنت.

لذا فإن سؤالنا يُعتبر أكثر تواضعاً: هل يمكن لتهديد الولايات المتحدة الأمريكية بأنها قد تتدخل في إطلاق الأسلحة النووية لدولة مارقة، أن يساعد على تصوير الأمر

كمواجهة نووية؟ في ما يتعلق بهذا السؤال، افترض أن قوة نووية مارقة لـديها قـدرة عـلى ضرب الدول القريبة (ولكنها عموماً غير قادرة عـلى ضرب الولايـات المتحـدة القاريـة). وتملك الولايات المتحدة قدرات هجومية قوية عبر الإنترنت (بصورة عامة)، ومن المؤكـد أن الترسانة النووية للدولة المارقة ليست بمنأى عنها. وعلى الرغم من أن الولايات المتحدة تتمتع بالهيمنة على التصعيد، فإن الدولة المارقـة تبـدو أشـد رغبـة مـن الولايـات المتحـدة الأمريكية في الوصول إلى حافة استخدام السلاح النووي، كـما أن الدولـة المارقـة (تعتقـد أنها) لديها أمور كبرى عرضة للخطر (أي، بقاء النظام). أضف إلى ذلك، أنها قد تتـصرف بطرق تُعتبر غير عقلانية من المنظور الغربي.

نقوم أولاً بنمذجة مواجهة بين دولتين، ثم بعد ذلـك نقـدِّم دولـة صـديقة تـدخلت الولايات المتحدة نيابة عنهـا. وتـدخل الولايـات المتحـدة هـذا الـسيناريو لتواجـه خيـار التصرف، وعندما تفعل ذلك تجازف بإمكانية أن تطلق الدولة المارقة سلاحاً نووياً. وسواء أكان ذلك صريحاً أم ضمنياً، فهو يُعدُّ أمراً ثانوياً؛ فالحسابات المعتادة تنطبق هنـا. فالدولـة المارقة ستكون أحسن حالاً إذا قاد تهديدها الولايات المتحدة الأمريكية إلى التوقـف، بيـنما ستكون الولايات المتحدة أحسن حالاً إذا تجاهلت التهديد ومضت قُدماً في ما قد فعلت في غياب التهديد، إذا كان بالإمكان إلغاء التهديد ولكنها لا يمكن أن تعلم أنه سـيكون أمـراً مؤكداً. وتدرك الدولة المارقة أنها إن استخدمت بالفعل الأسلحة النووية فقد تواجه انتقاماً عظيماً.[1]

إذا تـصرفت الولايـات المتحـدة الأمريكيـة (بنجـاح) في مواجهـة التحـذير، وإذا لم تستخدم الدولة المارقة الأسلحة النووية، تكون الولايات المتحـدة قـد حققـت أغراضـها وكسبت المواجهة كلها.[2] أما إذا تراجعت الولايات المتحـدة ونكـصت عـلى عقبيهـا، فـإن الدولة المارقة تفوز، أما إذا استخدمت الدولة المارقة أسلحتها النووية، وقامـت الولايـات المتحدة، كما هو مرجح، بالرد بالمثل، فـإن الدولـة المارقـة تخسر كثيراً، ولكـن الولايـات المتحدة تكون أيضاً أسوأ حالاً.[3]

المواجهات الثنائية الأطراف

في حال حدوث مواجهة تؤدي إلى كارثة نتيجة تنفيذ الطرفين تهديداتهما، ينبغي أن يسأل كل منهما: هل هذه التهديدات ذات مصداقية؟ إذا ظن أحد الطرفين أن الطرف الآخر سيستسلم، فإن الأمر يستحق الوقوف بثبات. لكن إذا اعتقد أن الطرف الآخر عنيد، فقد لا يملك خياراً جيداً سوى الإذعان والاستسلام. فتوقع العناد والتصلب مفيد، ولكن واقع العناد والتصلب كثيراً ما يكون انتحارياً.

ومن الملاحظ أن أساس العناد والتصلب يمكن أيضاً أن يكون ذاتياً، الأمر الذي يمكن القول إنه لا يستند إلى حقائق القضية. إذا كان أحد الطرفين مقتنعاً بأنه لن يدفع مطلقاً ثمناً عالياً لعناده، ويتصلب كثيراً، ويتصرف كما لو كان الأمر كذلك، فلا يمكن أن يجد الطرف الآخر أي راحة في حقيقة أن الطرف الأول لا يملك أي أساس تقني لذلك الاعتقاد. والاعتبار الوحيد هو ما إذا كان الطرف الأول يؤمن بالفعل بكل ذلك ويستعد للعمل وفقاً لإيمانه هذا، ويمكنه تجاهل المنطق الذي يهمس له بأنه لا أحد يمكنه الوثوق تماماً اعتماداً على معلومات هي موضع استفهام. يرى أحد الطرفين أن الاستعداد للتصرف على أساس المستحيل يبدو مثل الخداع. ولكي تستخدم القياس تخيل لعبة "الدجاج" Chicken game، التي يقوم فيها سائق إحدى السيارتين القادمتين بإلقاء عجلة القيادة خارج النافذة، فتدفع هذه الخدعة الخصم إلى الاختيار بين اصطدام مؤكد أو الابتعاد عنه (ومن ثم الخسارة). لكن عندما تكون عواقب الاصطدام أكبر من منافع الفوز، فإن هذه الاستراتيجية تكون خرقاء إذا كان هناك احتمال غير قليل بأن الطرف الآخر سيكون مصمماً على معاقبة المخادعين على حساب جميع القيم الأخرى. في القياس، لعل السائق الآخر يفضل الاصطدام على أن يخسر أمام المخادع [وبهذا فهو يفضل ألا يكون دجاجة؛ أي جباناً].[4] ولكن بصورة عامة، من الممكن أن تفلح استراتيجية العناد والتصلب، إذا كانت تتمتع بالمصداقية، ومادام الطرف الآخر لا يحمل الدرجة نفسها من التصلب.

لذا فإن الولايات المتحدة تعمل على صناعة اعتقاد (سواء بقول ذلك، أو بالتلميح، أو بترك الآخرين يستخلصون استنتاجاتهم) بأنه ليس بإمكان الدولة المارقة تنفيذ تهديداتها

النووية؛ أي إن الولايات المتحدة تتصرف كما لو أن ثمة خللاً في دورة القيادة والسيطرة، يحول دون الاستخدام الفوري للأسلحة النووية. وثمة حالة أقل من هذه، وهي أن تكون القيادة والسيطرة أقل تأكداً، والسلاح أشد ضعفاً، و/ أو كان نظام الإطلاق أقل دقة بكثير مما يخشى منه.[5] وعلى الرغم من أن التعطيل الدائم لنظام القيادة والسيطرة يُعدُّ توسعاً في الحرب عبر الإنترنت، فإنه أقل شطحاً في الخيال أن نتخيل أن الولايات المتحدة يمكن أن تؤجل استخدام أحد الأسلحة. ومع هذا، فإن ميزة مؤقتة يمكن أن تمنح الولايات المتحدة وقتاً لتتجاوز الخط الأحمر وتحظى بالتالي بفرض الأمر الواقع.

بهذا الوضع، تستعد الولايات المتحدة الأمريكية لتجاوز الخط الأحمر، في الوقت الذي تُفصح فيه عن ثقتها بأن الدولة المارقة لن تلجأ إلى الانتقام. وتنبع هذه الثقة من مزيج من قدرتها على الردع النووي، إضافة إلى قدرتها على إرباك القدرات النووية للدولة المارقة. ومن المرجَّح أن الدولة النووية المارقة لن تقرر الانتقام، وإذا ما قررت ذلك بالفعل فلعلها لن تستطيع الانتقام. وهذا المزيج، في هذه الحالة، هو ما يقلل من ترجيح فرصة الرد النووي إلى مستوى منخفض تماماً، إذا كان لدى الدولة المارقة ذرة من تعقّل. وحتى إذا طمأنت نفسها وغيرها في ما بعد بأن قدراتها النووية لم تمس، وكانت الولايات المتحدة الأمريكية قد تصرفت بالفعل، فإن المسؤولية تقع على كاهل الدولة المارقة لكي تستجيب لما يمكن أن يكون في الواقع صفقة ناجزة. وإذا فهمت الدولة المارقة المنطق قبل التلويح بأسلحتها النووية، فقد تختار عدم تصعيد التوترات قبل أن تجتاز الولايات المتحدة الخطوط الحمراء.

تتطلب هذه الاستراتيجية أن تؤمن الدولة المارقة بأن الولايات المتحدة الأمريكية عنيدة ومتصلبة، وتنبني، جزئياً، على إمكانية أن الولايات المتحدة تؤمن بأن بإمكانها استخدام العمليات عبر الإنترنت للقضاء على التهديد النووي. كما أنها تساعد أيضاً في ما لو أن الدولة المارقة لم تكن متيقنة تماماً من أن هذه الثقة في غير مكانها، علماً بأن هذه الاستراتيجية يمكن أن تنجح حتى إذا لم يكن ثمة أساس لهذه الثقة، ما دامت تعتقد أنه لا يمكن إقناع الولايات المتحدة بخلاف ذلك.

يمكن ملاحظة أن هذا الاعتقاد الضمني أو الصريح بوجود خلل معروف يُعتبر أوسع نطاقاً من الزعم بأن الولايات المتحدة الأمريكية سببت الخلل. ففي العديد من الجوانب يكفي أن الولايات المتحدة تعلم بالخلل، وأن الدولة المارقة لا تستطيع العثور عليه، أو لا يمكنها فعل شيء حياله خلال فترة الأزمة. ولعل الخلل موضع البحث قد تم إيجاده بوسائل خارج نطاق الفضاء الإلكتروني (كمخرب، مثلاً)، ولعله كان قيد التصميم طوال الوقت. لكن الخلل الذي يمنع إطلاق سلاح نووي يختلف عن الخلل الذي تستطيع الولايات المتحدة استغلاله لمنع إطلاق السلاح النووي. ويفقد الزعم الأول مصداقيته إذا كانت الدولة المارقة تستطيع إطلاق السلاح النووي، أما الآخر فيمكن أن يتجاوز الإطلاق وإن كان بشكل ضعيف، كما هو موضح في ما يلي.

على الرغم من أن الثقة بأن بإمكان الولايات المتحدة الأمريكية إحباط القدرات النووية لدولة مارقة من خلال الحرب عبر الإنترنت تماثل القدرة على فعل ذلك – مثلاً من خلال دفاع صاروخي فعال – فإن هناك فروقاً مهمة. ويمكن التدليل على فاعلية نظام الدفاع الصاروخي ضد صاروخ فعلي مكافئ في مستوى التطور (مثل امتلاك وسائل تساعد على الاختراق) لصواريخ الدولة المارقة. ولا تُعتبر مثل هذه الاختبارات حاسمة في الحرب عبر الإنترنت؛ لأن الحرب عبر الإنترنت عموماً تعتمد على وجود نقاط خلل وضعف لدى النظام المستهدف لا يدري صاحبه عنها شيئاً. ولا يمكن إجراء الاختبارات والبرهنة على مواطن الخلل هذه، إلا على نظم تعاني أنواع خلل معينة. وبمجرد أن يتم فهم طبيعة نقاط الخلل هذه يمكن إصلاحها أو الالتفاف عليها. وبعد ذلك تتعرض احتمالات أن تفلح مثل هذه الاختبارات في مواجهة ذلك الخلل بالذات لتراجع حاد. أضف إلى ذلك، أن وجود نظام دفاع صاروخي أمريكي وبعض خصائصه الأساسية يُعتبر معرفة عامة، ويمكن بذلك إدراجه في النقاش العام حول أرجحية – لنقُلْ – وقوع اشتباك ناجح خارج الغلاف الجوي، ومن هنا منشأ الحكمة في مواجهة دولة نووية مارقة. وعلى العكس من ذلك، فإن وجود الصفات الأساسية لقدرات الهجوم الأمريكي عبر الإنترنت لا يمكن سوى تخمينه؛ ويرجع ذلك في الغالب إلى ضرورة أن تكون قدرات الحرب عبر الإنترنت عالية الكفاءة لكي تبقى فعالة.

إن الإشارة إلى أن الدولة المارقة تعاني موطن خلل في الفضاء الإلكتروني لنظام القيادة والسيطرة النووية لديها، لا تسبب معضلة مؤداها إما أن تستخدمه وإما أن تخسره؛ فنقطة الضعف التي ساعدت على ظهور الخلل هي بالضرورة قد سبقت الأزمة، وكذلك على الأرجح سبقت اكتشاف الخلل واستغلاله. وهكذا نجد أن الدولة المارقة لا تتمتع بالقدرة، ومن ثم الدافع، لاستخدام الأسلحة النووية بصورة أسرع لكي لا تفقدها؛ لأن التهديد بهجوم عبر الإنترنت يعني ضمناً أن الدولة المارقة قد فقدتها (ولكن قد تستعيدها في ما بعد).[6]

ثمة تهديد أفضل، هو أن تقوم الولايات المتحدة الأمريكية بالرد على إطلاق فاشل للأسلحة النووية تماماً كما ترد على إطلاق نووي ناجح، حيث يوصل ذلك رسالة إلى الدولة المارقة بأنها يمكن أن تخسر الكثير بمحاولتها القيام بإطلاق السلاح النووي. وقد يقنع ذلك الدولة المارقة بالإذعان، إذا كان لدى الدولة المارقة أي أساس للاعتقاد أن مثل هذا الإطلاق قد لا ينجح. فالإخفاق يقود إلى هجمات مضادة تكون مدمرة كما هو الأمر في حال النجاح. والأسوأ من ذلك أن مصداقية الدولة المارقة ستتعرض لتراجع شديد. ولكن هل تستطيع الولايات المتحدة الأمريكية الانتقام لعملية إطلاق مخفقة؟ ثمة أمر واحد بالنسبة إلى إخفاق عملية الإطلاق بصورة ظاهرة؛ وهو أن الآخرين جميعاً يستطيعون قراءة النوايا. لكن إذا أخفق إطلاق صاروخ ما، فهل تستطيع الولايات المتحدة الانتقام، خاصة بأسلحة نووية، على أساس الأدلة التي ترد من الفضاء الإلكتروني فحسب، ويمكن بالتالي أن تكون ملفقة؟

في عالم الواقع، وفي الوقت الذي تتجه فيه الأسلحة النووية لأن تكون تناظرية، ونظم الإطلاق لأن تكون مزيجاً من التناظري والرقمي، فإن الروابط المبيحة لاتخاذ فعل، والتي تمنع إطلاق المنظومات النووية بالصدفة (ولاسيما تلك الموجودة في حوزة الدول النووية الجديدة)، هي روابط رقمية. وإذا كانت القوى النووية الأحدث عهداً تشتبه في أن الولايات المتحدة الأمريكية تسعى لإحباط استخدام السلاح، وذلك بالتدخل في العناصر الرقمية لنظم القيادة والسيطرة النووية، فقد تستنتج أن الولايات المتحدة الأمريكية قد

وجدت طريقة لاعتراض الروابط المبيحة لاتخاذ فعل. ولن يكون في مصلحة استقرار الدول أن تبدأ بتعطيلها خوفاً من العبث بها، فإذا قامت الدول بالفعل بتعطيل هذه الروابط، فإن ذلك يزيد من احتمالات إطلاق هذه الأسلحة عن غير قصد. ومن هنا، نجد في عالم الواقع أن التهديد باستخدام الهجمات عبر الإنترنت ضد العمليات النووية للدول المارقة تنتج عنه مضاعفات مهمة وسلبية على المدى البعيد.

تعطيل قدرات في مقابل إحباط تهديد

يختلف إحباط قدرة دولة مارقة على التهديد باستخدام الأسلحة النووية عن إحباط قدرتها على استخدام هذه الأسلحة؛ فإحباط تهديد يتطلب إسقاط الثقة عن الخصم؛ بحيث لا تعمل القدرة الكامنة وراء التهديد، وبحيث تتم المجازفة بأن تقوم الدولة المارقة، بعد إنذارها بهذه الطريقة بإعادة فحص نظم القيادة والسيطرة النووية لديها، وإصلاح الخلل أو الالتفاف حوله (مثلاً، السماح بمزيد من الفرص للسيطرة "اليدوية" على نظام إلكتروني مصاب بالخلل). وبذلك، فإن تلميحات اليوم يمكن أن تقلل احتمالات التسوية الفعلية مع مرور الوقت.

وعلى العكس، فإن امتلاك قدرة الهجوم عبر الإنترنت وعدم التلويح بها لن يخفف الضغط عن الولايات المتحدة للانسحاب من إحدى الأزمات التي تقوم فيها دولة مارقة بالتلويح بأسلحة نووية. قد يأتي مثل هذا الضغط من معارضة داخلية أو حلفاء أو محاورين محترمين أو - كما هو وارد في ما بعد - من الدولة نفسها التي تدخلت الولايات المتحدة لأجلها للدفاع عنها ضد الدولة المارقة. عندئذ، فإن امتلاك القدرة ليس عديم الفائدة، حتى على الصعيد العام. فإذا حصلت القيادة الأمريكية على الثقة الكافية من خلال معرفة أنه من الممكن تعطيل القدرات النووية للعدو، فقد يستنتج الآخرون أن الولايات المتحدة تملك أسباباً كافية تبرر ثقتها، حتى إذا لم يتم الكشف عن هذه الأسباب، ويرى البعض أن هذا جيد بدرجة كافية.

إن التوتر الكائن بين كسب مواجهة من خلال الإبلاغ عن نقطة ضعف الخصم وبين الحد من أضرار الحرب باستغلال نقطة ضعف الخصم، يدل على الحاجة إلى وزن

الاحتمالات التي ترجِّح أن الدولة المارقة ستستخدم أسلحتها. فإذا كانت أرجحية الاستخدام منخفضة (مثلاً، لأن من المتوقع أن يؤدي التصلب الأمريكي إلى النتيجة المطلوبة)، فإن ذلك يبرر المزيد من التلميحات، أما إذا كانت احتمالات الاستخدام عالية فإن مزيداً من الصمت هو الخيار الأفضل. وإذا كانت الدولة المارقة تفهم بهذا القدر، فسوف تستنتج أنه، إذا كانت الولايات المتحدة الأمريكية تسعى لتنقل رسالة مفادها بأنها تعرف سراً، فإنها – أي الولايات المتحدة – تؤمن بضعف احتمالية الاستخدام الفعلي؛ لأنها تستطيع في الواقع ردع الدولة المارقة. وهذا يُسهم في تعزيز الرسالة التي تفيد بأن نقاط الخلل في الأسلحة النووية لدى الدولة المارقة لا بد من أخذها مأخذ الجد، أو على الأقل بأن الولايات المتحدة تأخذها مأخذ الجد.

قد تسعى الدولة المارقة إلى تكذيب خدعة الحرب عبر الإنترنت

افترض أن الدولة المارقة، بعد أن نظفت نظم القيادة والسيطرة النووية لديها، تنجح في إزالة كل الشكوك حول مصداقيتها، على الرغم من صعوبة التيقن من أن الاستخبارات الأمريكية (العليمة والبصيرة على ما يبدو) لا تعرف شيئاً عن النظم النووية للدولة التي غفلت عنها (تذكر مثال ستكسنت)، وبكونها تعلم أن المفاجآت في الفضاء الإلكتروني تُعتبر مفاجئة في التفاصيل، ومع ذلك يتكرر حدوثها مراراً.

لو أن الأساس المتصوَّر للثقة الأمريكية كان يتناقض مع ما عرفه القادة عن نظام القيادة والسيطرة النووي، فقد يكون من الصعب مع هذا إقناع الدولة المارقة بأن الولايات المتحدة الأمريكية شعرت حقاً بالثقة. ومن شأن هذا المنطق أن يدفع الدولة المارقة إلى إقناع الولايات المتحدة بأن قدرتها على تنفيذ التهديد النووي لن تتضرر بهجوم عبر الإنترنت.

ولكن كيف؟ تتمثل إحدى الطرق في الكشف عن شيء ما بشأن قيادتها وسيطرتها بما يدل على أن أساس الاعتقاد الأمريكي وهمي. لكن كلما كشفت أكثر عن قيادتها وسيطرتها أعطت مزيداً من المعلومات للمحاربين المحترفين عبر الإنترنت في الولايات المتحدة

(وجميع الدول الأخرى) للعمل معها سعياً وراء معرفة موضع خلل جديد. وقد يعطي مثل هذا الكشف معلومات مفيدة للقوات الخاصة المعادية، وكذلك معلومات للكشف عن الأهداف إلى القوات الجوية المعادية. ولعله يحدث بعض التردد إذا شعرت الدولة المارقة بأن كشف الأسرار عن قيادتها وسيطرتها يمكن أن يُطلع الجماهير الداخلية (مثل، بعض أعضاء المؤسسة العسكرية) على أشياء تفضل قيادتها ألا يعرفوها.

أما الطريقة الأخرى، فهي القيام بعملية إطلاق وتفجير ناجحين. ومن شأن النجاح إلغاء إمكانية أن يكون الخلل الناشئ أو المكتشف في القيادة والسيطرة منتشراً وذاتي المنشأ. ومن المؤكد أن عملية إطلاق فاشلة، تعطي إشارة بالاستعداد لاستخدام هذه الأسلحة بطرق لا يدل عليها مجرد امتلاك هذه الأسلحة. ولكن عملية إطلاق ناجحة لا تلغي إمكانية كون استغلال الخلل أمراً يمكن أن تفعّله الولايات المتحدة الأمريكية كلما أرادت، أو أمراً لا يظهر إلا في ظل ضوابط إطلاق معينة (مثلاً، إذا كانت نقطة هدف الصاروخ موجودة في أراضٍ لا تريد الولايات المتحدة الأمريكية ضربها). ورغم ذلك، كان بإمكان الولايات المتحدة أن ترفض اعتراض الضربة النووية اعتقاداً منها أن النتائج لا تحمل معها عواقب خطيرة (مثل أن تكون عملية إطلاق استعراضية في أراضي الدولة المارقة). وهذا يترك مع ذلك الباب مفتوحاً أمام إمكانية أنه إذا كانت عملية الإطلاق ذات أهمية بالفعل، فإن بإمكان الولايات المتحدة إيقافها. وإذا كان الأمر كذلك، فلايزال بإمكان الولايات المتحدة الحفاظ على تصميمها بعبور أي خط أحمر تضعه الدولة المارقة.

سيكون على الدولة المارقة، بناء على توقعها ذلك كله، إثبات رؤيتها من خلال ضربة نووية تؤدي إلى إحداث النتائج (1) أنها أضعف من أن تستحق رد فعل مدمراً من الولايات المتحدة الأمريكية، ولكنها (2) قوية بما يكفي لتجاوز ما يمكن للولايات المتحدة التسامح معه باتزان ورباطة جأش (لاحظ التشابه مع فاصل الغضب-الخوف الذي سبق بحثه). وسوف يحمل ذلك مخاطر أقل للدولة المارقة النووية (لأن الانتقام لن يتبع ذلك)، ولكنه سيضعف أساس الثقة لدى الولايات المتحدة (لأنها لو استطاعت إيقاف الضربة لفعلت ذلك). ومن الأمثلة الممكنة على ذلك رأس حربية غير نووية مركبة فوق نظام

إطلاق نووي يتم إطلاقها نحو وجهة يمكن أن يؤدي الانفجار فيها إلى قتل عدد كبير من الناس، لو كان نووياً. نظرياً، قد لا تكون الولايات المتحدة تدري أن الضربة غير نووية إلى أن يحدث الانفجار. ورداً على ذلك، يمكن أن تشير (وعلى الأرجح تلمّح) إلى أن مستوى المعرفة المطلوبة لولوج دورة القيادة والسيطرة النووية كاف تماماً للتمييز بين ضربة نووية وأخرى تقليدية. وثمة مسألة أكثر عملية، إذا لم تضع الولايات المتحدة خطاً تحبط عنده أي ضربة، والخط الذي تنتقم عنده انتقاماً مدمراً، فكيف تعرف الدولة المارقة إذا ما كان ثمة ضوء يميز بين الاثنين؟

وعلى العكس من ذلك، فإن ضربة استعراضية تقليدية (1) تعطي الآخرين مبرراً للتشكيك في مدى الحاجة إلى عملية الاستعراض (وربما تؤكد أن الشائعات لها أساس)، و(2) تستهلك صاروخاً واحداً على الأقل من مجموعة صغيرة، و(3) قد لا تعالج الشك بأن ثمة خللاً في جهاز الاندماج في السلاح النووي (التركيبة الفيزيائية للرأس النووي) لايزال نشيطاً.

إن الاستراتيجية الأمريكية تتطلب أيضاً دراسة ما إذا كان بإمكان الدولة المارقة إثارة قضية تدل على أن نظمها النووية تعمل. قد لا يكون لدى الدولة المارقة دائرة انتخابية لكي تجيب أمامها، أما الولايات المتحدة فيوجد لديها هذا النظام، ولاسيما إذا كانت أرواح الأمريكيين في خطر، وحتى أبعد من ذلك إذا كان عملها الحربي يشمل حلفاء (تتم مناقشته في ما بعد). وحتى إذا عبّرت الولايات المتحدة عن الثقة في أقوالها وأفعالها، فكيف تبلّغ الآخرين عن أساس ثقتها؟ وماذا تكشف لتُظهر ذلك؟ عند التأمل في هذا السؤال، يتعين على الخبراء الاستراتيجيين معرفة أن الدولة المارقة قد تناقض أي عملية إفشاء، وحتى إذا كانت المعلومات التي يتم الكشف عنها صحيحة، فيمكنها معالجتها في الوقت المناسب إذا كان الزعم محدداً بشكل يكفي لتحديد أين يمكن البحث عن موطن الخلل.

هل سيكون من المفيد إقناع الدولة المارقة بأن الولايات المتحدة بـ"إمكانها" امتلاك مثل هذه السيطرة، أفضل من إقناعها بأن الولايات المتحدة "تعتقد" أنها تملك تلك السيطرة؟ سوف يساعد ذلك في ما لو كان قادة الدولة المارقة مقتنعين بأن الولايات

المتحدة "يمكنها" امتلاك مثل هذه السيطرة، "إذا" كانوا يعرفون أنهم لا يفهمون البرامج الموجودة في نظام القيادة والسيطرة النووية لديهم بما فيه الكفاية ليعلموا أنه لم يكن معرَّضاً للخطر. وتتمثل إحدى مزايا الإقناع في أنه إذا اعتقد قادة الدولة المارقة أنهم سيُحدثون ضجة، فسوف يجدون أنهم يسعون للخداع، وسوف يعالجون الأزمة بمزيد من التردد. وإذا كانوا يخشون أن تكتشف الولايات المتحدة ترددهم، فقد يفكرون في أنها ستعالج الأزمة كما لو أن الدولة المارقة تسعى للخداع، الأمر الذي يضع الدولة المارقة من جديد في وضع الخسارة إذا أذعنت، وفي وضع أسوأ إذا قامت بشن هجوم نووي.

ومن المفارقة أنه كلما رغبت الولايات المتحدة في الإعراب عن ثقتها، كانت مثل هذه الثقة أدنى مصداقية. وإذا كانت الولايات المتحدة واثقة حقاً من أن بإمكانها منع هجوم نووي، فلن يهمها كثيراً أن تشعر الدولة المارقة بخلاف ذلك. وأياً كان الأمر، فلن يحدث شيء سيئ. وهكذا نجد أن الرغبة الملحة في إظهار الثقة تعني ضمناً أن الولايات المتحدة تهتم بما تفكر فيه الدولة المارقة، الأمر الذي يعني أن ثقتها ليست مكتملة.

هل يسهم التلويح بهجوم نووي في إحباط استخدام الأسلحة النووية أو التهديد باستخدامها؟

هل يُعتبر التلويح بقدرات الهجوم عبر الإنترنت مفيداً عندما يكون ثبات الولايات المتحدة قضية غير واردة أو ملائمة؟ ولعل الأمثلة تشمل استبعاد ضربة نووية من جانب واحد (مثلاً، مفاجئة تماماً) أو إقناع دولة مارقة بعدم إثارة الرهان النووي أو وضع نفسها في موقف تشعر فيه أنه لا خيار لديها سوى استخدام الأسلحة النووية. وفي الحالة الأخيرة، يمكن أن ينتهي موقف الإصرار الأمريكي، حتى إذا تم دعمه بالتلويح بقدرات الهجوم عبر الإنترنت، إلى نتيجة سيئة. فهل ثمة فائدة في التلميح لدولة مارقة بأن قيادتها وسيطرتها النووية تحتوي على نقاط ضعف وخلل، في الوقت الذي لا تكون فيه تحت ضغط ملح لاستخدام تلك القدرة (كما سيكون الأمر لو حاولت منع الولايات المتحدة من تجاوز خط أحمر)؟

لسوء الحظ، تم تنبيه الدولة المارقة السابقة إلى احتمال وجود نقاط خلل في نظام القيادة والسيطرة النووي لديها، مما منحها مزيداً من الوقت لإيجادها وإصلاحها.[7] أما إذا كان من الممكن للدولة المارقة بعد ذلك أن تقنع نفسها - بعد الإصلاح - بأنه قد تم إصلاح نظام القيادة لديها بالفعل، فهذه قضية مختلفة. ومن الواضح أن عدد المشكلات في هذا النظام أقل. فإذا كان ثمة ظن بأنه كان يعاني مشكلة واحدة من قبل، فهو لا يعاني شيئاً الآن، ومن ثم يعود بثقة إلى الحافة. كيف ستعرف أنها بدأت بنقطة خلل واحدة قابلة للاستغلال؟ لعل عملية إيجاد نقطة خلل واحدة لا تمثل سوى إشارة فحسب إلى أن لديها عدة نقاط خلل يمكن استغلالها مبدئياً. وهكذا نجد أن العدد المتوقع لنقاط الخلل القابلة للاستغلال يمكن على الأغلب أن يكون أكبر بعد إزالة نقطة واحدة من قبل.[8] وعلى العكس، إذا بحثت الدولة المارقة ولم تعثر على نقاط خلل، فقد تستنتج أن الولايات المتحدة الأمريكية كانت تخادع، أو أن محاربي الإنترنت الأمريكيين كانوا على مستوى من الذكاء والدقة جعل من الصعب اكتشاف الثغرة ذات الصلة حتى بعد البحث المضني.

الأطراف الصديقة الأخرى تزيد من التعقيدات

يمكن أن تسهم الأطراف الصديقة الأخرى التي تملك حق الاعتراض على إجراءات الولايات المتحدة الأمريكية في تعقيد عملية التلويح بالقدرات الأمريكية على الهجوم عبر الإنترنت من أجل تقوية الموقف الأمريكي، ولهذه الأطراف سبل عديدة لممارسة حقها في الاعتراض، وليس أقلها حرمان القوات الأمريكية من دخول أراضيها. وعلى الرغم من استطاعة القوات المسلحة الأمريكية القيام بالعمليات من البحر أو من قواعد جوية بعيدة، فإن اعتراض الطرف الثالث على الإجراءات الأمريكية المنتظرة يمكن أن يحدّ من الأسس المنطقية المبدئية الأمريكية لأي عمل عسكري في المنطقة.

وعلى الرغم من العداء الذي تحمله الأطراف الصديقة الأخرى ضد الدولة المسلحة نووياً، واستعداد أكبر ذي صلة لرؤيتها ذليلة مهانة، وربما منزوعة السلاح، فقد تصاب بالذعر من خديعة الحرب عبر الإنترنت. أولاً، من المرجح أن تكون هي ومواطنوها

عرضة لخطر أكبر، نتيجة للوجود ضمن مدى المنظومات النووية للدولة المارقة. وثانياً، أنها تعرف أقل مما تعرفه الولايات المتحدة الأمريكية حول قدرات الحرب عبر الإنترنت التي تملكها الولايات المتحدة وكيف يمكن استخدامها. ونتيجة لذلك، نجد أن الأطراف الأخرى تملك ثقة أقل بأن مثل هذه الخطط ستنجح.

لن يفوت أيٌّ من هذا انتباه الدولة المارقة التي يمكن أن تستنتج أنه لا داعي لأن تنظر شذراً إلى الولايات المتحدة إذا كان بإمكانها تخويف الطرف الثالث. وحتى إذا وقف الطرف الثالث مع الولايات المتحدة لتشكيل جبهة موحدة ضد الابتزاز النووي، فسوف يواجه فترة صعبة مظهراً الثقة المطلوبة لاتخاذ موقف، مما يزيد من جرأة الدولة المارقة التي تتصور أن تهديداتها ستصدّع الجبهة الموحدة على الأغلب.

قد تحتاج الولايات المتحدة الأمريكية إلى خيارات لإبقاء الطرف الثالث ضمن الصف إذا كان ذلك سيدعم قدراتها في الحرب عبر الإنترنت لتقوية موقف التحالف في المواجهة. تستطيع الولايات المتحدة، على سبيل المثال، أن تطلب إلى حليفتها أن تقف بثبات وتعوّل على تأكيد الولايات المتحدة على هشاشة النظام النووي للدولة المارقة، مع تهديد غير معلن على صيغة "وإلا.." يُضاف كتعزيز للإجراء. وثمة خيار أكثر تساهلاً يتمثل في إقناع الطرف الثالث بأن مظهر الثبات سيردع الدولة النووية المارقة. لكن هذه المقولة تكون منطقية بالدرجة نفسها مع، أو دون، تهديد مضاد بالحرب عبر الإنترنت.

لعل قيادة الطرف الثالث تشعر بالطمأنينة بتأثير الثقة الأمريكية، ولكنها أيضاً يمكن أن تستشير ضباط قواتها المسلحة الذين لديهم تواصل يومي كاف مع نظرائهم الأمريكيين لكي تقيس بشكل دقيق حجم الثقة لدى القادة الأمريكيين بقدرتهم على إحباط التهديد النووي من جانب الدولة المارقة. وعلى الرغم من ذلك، أو ربما بسبب ذلك، قد يرغب الطرف الثالث في بعض الأدلة على أن بإمكان الولايات المتحدة أن تفعل ما توحي بأنها تستطيع فعله. ما الذي يمثل هذه الأدلة؟ وما الذي ترتاح الولايات المتحدة لإظهاره للطرف الثالث؟

إن أي إجابة غير "ثقوا بي في ذلك" تفترض سياسة أمريكية أكثر انفتاحاً، بشأن الكشف عن قدرات هجومية للدول الأخرى، مما تبدو عليه الآن.[9] قد تسهم أزمة في نشوء مخاطر جديدة مرتبطة بتبادل المعلومات. إذا كان ثبات الموقف يتطلب من القوات الموالية للولايات المتحدة أن تُظهر الإيمان بقدرة الأخيرة على إحباط تهديد نووي، فإن أولئك الذين يشعرون بالتوتر حيال الإقدام على مثل هذه المخاطر الهائلة، والمشككين بقوة الحرب عبر الإنترنت، أو خصوم الولايات المتحدة داخل حكومة الدولة الحليفة، سيكون لديهم الحافز للاحتجاج بأنه قد تم تضخيم القدرات الأمريكية في الحرب عبر الإنترنت. كما أنه لا يمكن إغفال اختراق دول الطرف الثالث من قبل عملاء الدولة النووية المارقة.

بالمناسبة، ثمة منطق مشابه ينطبق إذا كان الطرف الثالث داخلياً (مثل، الكونجرس الأمريكي، وصناع الرأي، وعامة الشعب). وكلما كان دور قدرات الحرب عبر الإنترنت أكثر بروزاً بالنسبة إلى القدرات الانتقامية في إيضاح أسباب ثبات موقف الولايات المتحدة، كان الطلب أكبر على إيضاح أسباب ضمان مثل هذه الثقة. قد يكون من مصلحة الدولة المارقة – في الواقع – أن تحتج بأن قدرات الحرب عبر الإنترنت هي الأساس الأولي لثبات الموقف الأمريكي، وذلك للضغط على الولايات المتحدة لعرض ما يمكنها فعله.

إذن، ما الذي يمكن إيضاحه؟ يمكن الإيضاح لممثلي حكومة الطرف الثالث في الوقت الحقيقي كيف يعمل نظام القيادة النووي للدولة المارقة. والمأمول هو أن تقبل هذه الدول في الطرف الثالث صحة ما يتم إيضاحه لهم (وأن الدولة المستهدفة لا تدير فخاً لتقصي المحاولات غير المصرحة للولوج إلى شبكاتها من أجل خداع المهاجمين). وثمة عرض أفضل يتمثل في تعديل شيء في نظام القيادة النووية للدولة المارقة يظهر أثره على الفور بحيث يستطيع الطرف الثالث ملاحظته بصورة مستقلة، ومن ثم، يأمل أنهم سيقبلون حقيقة أن الاستغلال ينطبق على جميع نظم القيادة النووية التابعة للدولة المارقة.[10] وهكذا، وكحد أدنى، فإن على الولايات المتحدة الأمريكية أن تشارك في معلومات مفصلة جداً عما تعرفه عن نظام القيادة النووية للعدو يتم من خلالها، وللأسف، كشف المصادر والطرق.

وبهذا الصدد، يتعين أن تنطبق التحذيرات المعتادة. قد تكون كلها خدعة، وقد يخفق الاستعراض، حتى لو كان حقيقياً. وقد ينجح، وببساطة، قد لا يتم تصديقه. وقد يشعر الطرف الثالث أن الدولة النووية المارقة قد أخفت أشياء كثيرة تتعلق بنشاطاتها. إن ذلك يساعد إذا فهمت الولايات المتحدة الطرف الثالث جيداً وبدرجة تكفي لتعرف ما الذي سيفاجئه ويسرّه، ومن ثم تفعل شيئاً يطابق ذلك تماماً.

ويتوقف هذا كله على فن الممكن في عالم يكون فيه للدولة النووية المارقة كل حافز وكل وسيلة للحفاظ على القيادة والسيطرة على معظم معداتها العسكرية المهمة.

الخلاصة

يهدف التلويح بقدرات الهجوم عبر الإنترنت في أزمة نووية إلى تعزيز الثقة الأمريكية بعدم الإذعان قبل حدوث تهديد خطير. وكلما زادت الولايات المتحدة الأمريكية من إيمانها بأن بإمكانها اختراق نظام القيادة لدولة نووية مارقة، زادت احتمالات أن تستطيع الولايات المتحدة الاحتفاظ بحريتها في التصرف في أي مواجهة. وسوف تفهم الدولة المارقة أن عليها الاختيار بين القيود والإبادة؛ لأنها لن ترى إمكانية لإذعان الولايات المتحدة الأمريكية. وكلما زاد إيمان الولايات المتحدة بأن الدولة المارقة ستتجاهل حتى التهديدات ذات المصداقية بهجوم عبر الإنترنت على نظام القيادة والسيطرة النووية لديها، قلت القيمة التي تجدها الولايات المتحدة في جعل مثل هذا التهديد بهجوم عبر الإنترنت ذا مصداقية (لأن الصراحة حول كيفية نجاح الهجوم عبر الإنترنت ستجعل من السهل مواجهته). وكلما كان إخفاء الولايات المتحدة تفاصيل قدرتها على الحرب عبر الإنترنت أفضل، زاد احتمال أن تقوم الدولة المارقة بإعداد تلميحات عكسية وتحدد بالضبط ما يمكن أن تستغله. وبذلك يكون من الأفضل إحباط الدولة النووية المارقة إذا ما استخدمت الأسلحة النووية.

وعلى العكس، فمن الممكن أن تقرأ الدولة النووية المارقة "التلميحات" عن القدرات الأمريكية باعتبارها تكتيكاً للرعب، وهو أمر لن تستخدمه الولايات المتحدة الأمريكية لو أنها استخدمت بالفعل – وفكرت باستخدام – تلك القدرات. وقد تستنتج الدولة النووية

المارقة أن لدى الولايات المتحدة قدراً كبيراً من الثقة (عن جدارة) في قدراتها إلى درجة أنها اعتقدت أن "التلميحات" ستكفي لردعها.

قد تحصل فائدة ثانوية من حقن الدولة النووية المارقة بالشكوك قبل الأزمة؛ إذ قد يردعها ذلك عن التمادي في الأزمة بحيث يتعذر عليها التراجع من دون فقدان كبير لماء الوجه وعدم تجاوز الخط الذي يطغى عنده يقين الإحراج الكبير على الاحتمال (الضعيف المتصور) لتفادي الانتقام.

ولكن ماذا لو أن النجاح في مواجهة نووية تطلّب تعاون دولة هي عبارة عن طرف ثالث تكون عادة أكثر عرضة للأسلحة النووية الموجودة لدى دولة مارقة من تعرض الولايات المتحدة لها؟ إذا كانت الوعود والتهديدات المبطنة لا يمكنها إبقاء الدولة التي هي طرف ثالث ضمن صف التحالف فقد تطلب هذه الدولة من الولايات المتحدة إثبات كل ذلك. ومع هذا، فإن مثل هذا البرهان قد لا يتوافر من دون عملية استعراض وإثبات، فهذه العملية إذا أخفقت سوف تنزع المصداقية من جميع مصادر الثقة الأخرى. أما إذا نجحت فقد تكون بمنزلة تنبيه للدولة النووية المارقة التي ستعمد عندئذ إلى إصلاح الخلل الذي سمح بوجود الثغرة. أضف إلى ذلك، أن الطرف الثالث يمكن أن يسرّب هذه المعلومات، ولاسيما إذا كان ثمة أشخاص لدى الدولة التي هي طرف ثالث أو لهم صلة بها، ويريدون نزع المصداقية عن حجج الولايات المتحدة.

وعلى الرغم من ذلك، فإن هناك هشاشة في مبالغة الولايات المتحدة الأمريكية في الاعتماد على قدرات الهجوم عبر الإنترنت لتعزيز رفضها الإذعان لتهديد نووي. وثمة عنصر مهم، وربما ضروري، في ذلك التكتيك؛ وهو عجز الدولة المارقة عن اكتشاف كيف سيكون ذلك (لأن فهم تفاصيله يمكن أن يؤدي إلى إلغاء مثل هذه القدرات). ولكن يتعين على الدولة المارقة مع هذا أن تدرك أن الأمر يمكن أن يكون كذلك إن كانت ثمة إمكانية لأن يساعد التلويح بقدرات الهجوم عبر الإنترنت الولايات المتحدة الأمريكية على إدارة الأزمة. وباختصار، يجب أن تثق الدولة النووية المارقة بما لا تستطيع رؤيته، وذلك بناء على سمعة المؤسسة العسكرية الأمريكية.

الاستنتاجات

من شأن التلويح بالقدرات عبر الإنترنت أن يفعل ثلاثة أمور: إعلان القدرات، والإيحاء بإمكانية استخدامها في ظرف معين، وإيضاح أن مثل هذا الاستخدام سيُحدث أضراراً حقيقية. في حقبة المواجهة النووية الأمريكية - السوفيتية، كانت دلائل الاستخدام واردة جداً؛ إذ كان امتلاك الأسلحة النووية واضحاً، وعواقب استخدامها مفهومة تماماً. وهذا الأمر لا ينطبق على الأسلحة في الفضاء الإلكتروني؛ ذلك أن الامتلاك ليس واضحاً، والقدرة على إحداث أضرار حقيقية هي موضع جدل. وحتى إذا تم استعراضها والبرهنة على وجودها وإمكانية استخدامها؛ فما نجح بالأمس قد لا ينجح اليوم. ولكن الصعب لا يعني المستحيل.

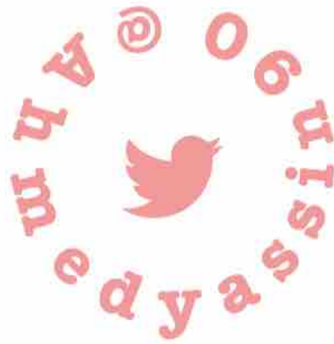
ولعل الدعاية لقدرات الهجوم عبر الإنترنت ستكون مفيدة؛ إذ يمكن أن تمثل دعماً لاستراتيجية الردع، كما يمكن أن تصرف الدول الأخرى عن التسبب بالأذى التقليدي، أو تصرفها حتى عن الاستثمار في قدرات يمكن أن تسبب الأذى والضرر. وقد تقلل من ثقة الطرف الآخر بمصداقية معلوماته، أو قيادته وسيطرته، أو منظومات أسلحته. وقد تساعد في حال المواجهة النووية على بناء نفوذ يُقنع الدول الأخرى بأن الملوِّح باستخدامها سيصمد، وبذلك تُقنع الدول الأخرى بالإذعان.

ومع ذلك، فإن إثبات مثل هذه القدرات ليس بالأمر السهل، حتى إذا وُجدت؛ فقدرات الفضاء الإلكتروني لا تظهر إلا في علاقتها مع هدف محدد، والذي يجب معرفة نطاقه ومداه كي يتم فهمه. وبإمكان محاربي الفضاء الإلكتروني إيضاح قدرتهم على اختراق النظم، ولكن اختراق هذه النظم لا يضاهي تعطيلها من خلال طرق مفيدة. وبما أن الهجمات عبر الإنترنت تُعدُّ في الأساس أسلحة أحادية الاستخدام، فإنها تتضاءل مع استعراضها. وقد يكون من الصعب إقناع أصدقائك بأن لديك مثل هذه القدرات عندما تكون الشكوك في مصلحتهم.

علاوة على ذلك، فإن التلويح يمكن أن تكون له نتائج عكسية. ذلك أن الترويج للقدرة على الرد في الفضاء الإلكتروني، يمكن أن يوصل رسالة مفادها الابتعاد عن العنف. وقد يؤدي ادّعاء القدرة على تغيير الواقع إلى إقناع الآخرين بتوجيه اللوم إلى المدّعي إذا كان الواقع غير ملائم. أما التدخل في القيادة والسيطرة لدى الآخرين فيمكن أن يسمح لهم بتبرير قواعد الاشتباك التي تجعلهم يتخلون عن مسؤوليتهم عن تابعيهم.

هل يتعين على الولايات المتحدة الأمريكية أن تُشعر العالم بأنها تمتلك قدرات الهجوم عبر الإنترنت، وبأنها تعرف كيف تستخدمها؟ ليس ثمة حكمة واضحة في مثل هذا المسار. فلا توجد سوى أدلة ضئيلة على أن الآخرين يتصرفون؛ لأنهم لا يصدّقون أن الولايات المتحدة تملك قدرات عبر الإنترنت أو تستطيع تطويرها. وبالمقابل، تعتمد المكاسب من مثل هذا التلويح بهذه القدرات على السياق، ويمكن أن تكون مثيرة للمشكلات حتى حينئذ.

إن التلويح بالهجوم عبر الإنترنت ينطوي على أمور مشجّعة وعلى مخاطر أيضاً، في الحالتين التقليدية والنووية على حد سواء. ولا ضير في التفكير الجدي في طرق تستطيع الولايات المتحدة الأمريكية من خلالها تعزيز قدرتها على استغلال ما يراه الآخرون قدرات وطنية. ومن المؤكد أن فيروس ستكسنت قد أقنع آخرين بأن الولايات المتحدة تستطيع فعل الكثير من الأمور المتطورة في الفضاء الإلكتروني (بغض النظر عما إذا كانت الولايات المتحدة قد ساهمت بشكل عملي في ستكسنت أم لا). وسوف يتطلب هذا الجهد كثيراً من التحليل والتخيل؛ لأن الخيارات المختلفة التي عُرضت في هذه الدراسة لا يُعتبر أي منها ناجحاً بشكل واضح. ذلك أن التلويح خيار قد لا ينجح أيضاً، فهو ليس ترياقاً لكل العلل. ومن المستبعد أن يساعد التلويح على نجاح الردع إذا كانت عناصر الردع الأخرى (إرادة شن الحرب أو القدرة على إلصاق التهم بالنسبة إلى الخطوط الحمراء المرسومة في الفضاء الإلكتروني) ضعيفة.



تصوير
أحمد ياسين
تويتر
@Ahmedyassin90

الهوامش

الملخص

1. لاحظْ أن استعمال كلمة "تلويح" هنا يهدف إلى استلهام صور المحاربين الذين يبرزون أسلحتهم (ومن ثمّ قدراتهم) قبل المعركة، من قبيل التحذير، وليس من قبيل إشهار مسدس بقصد الإجرام وتهديد أحد الضحايا.

الفصل الأول

1. لاحظْ أن استعمال كلمة "تلويح" هنا يهدف إلى استلهام صور المحاربين الذين يبرزون أسلحتهم (ومن ثمّ قدراتهم) قبل المعركة، من قبيل التحذير، وليس من قبيل إشهار مسدس بقصد الإجرام وتهديد أحد الضحايا. [هكذا جاء هذا الهامش مكرراً في النسخة الأصلية من الدراسة عند ورود كلمة "تلويح" في كلٍ من الملخص والفصل الأول. المحرر].

2. لا تنسجمُ صراحةُ التهديدِ بالضرورة مع كيفية التصريح بإحدى القدرات بوضوح، فمن الممكن أن تكون واضحاً جداً حول امتلاك إحدى القدرات دون رسم خطوط حمراء (الخط الأحمر هو حدٌّ تضعه الدولة وتشعر بعده بأن عليها اتخاذ إجراء). ويمكن للمرء إطلاق تهديد صريح بناءً على قدرة يتم عرضها باستحياء، ولكن بمزيد من الصعوبة نوعاً ما.

3. بين العديد من المصادر التي تؤكد أن الجريمة سائدة في الفضاء الإلكتروني، انظر:

Jonathan Masters, "Confronting the Cyber Threat," New York: Council on Foreign Relations, May 23, 2011; Richard J. Harknett, John P. Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 1, November 11, 2010; and Eric Sterner, "Stuxnet and the Pentagon's Cyber Strategy," Arlington, Va.: George C. Marshall Institute, October 13, 2010.

4. مع ذلك، عندما سُئل الجنرال ألكساندر عما إذا كانت الولايات المتحدة قد امتلكت من قبل «قدرات مثبتة في الفضاء الإلكتروني بطريقة من شأنها أن تقود إلى ردع الأعداء المحتملين»، أجاب: «ليس بأي طريقة مهمة»، انظر:

Keith Alexander, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," statement to the U.S. Senate Committee on Armed Services, April 15, 2010, p. 21.

5. انظر:

George H. Quester, *Deterrence Before Hiroshima*, Piscataway, N.J.: Transaction Publishers, 1986.

لاحظ أن بالدوين Baldwin كان يتحدث عن أكثر من اثني عشر عاماً، وعن العديد من أجيال الطائرات بعد آخر استخدام للقوة الجوية ضد عدو متطور. ومع هذا، فقد أثبتت معركة بريطانيا في ما بعد أنه بمجرد أن واجهت الدول قاذفات حقيقية، كانت الأضرار أقل مما كان متخوَّفاً منها، ولم تتجاوزها دائماً.

6. ينسجم مع تقرير المؤلف السابق حول الردع، انظر:

(Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: R AND Corporation, MG-877-AF, 2009),

وتشير كلمة "ردع" فقط إلى الردع بواسطة العقاب، ولا تشمل الردع بالحرمان.

الفصل الثاني

1. يمكن الاطلاع على نسخة سابقة من النقاش الأساسي لهذا الفصل في مقال المؤلف:

"Wringing Deterrence from Cyberwar Capabilities," in Richmond M. Lloyd, ed., *Economics and Security: Resourcing National Priorities*, proceedings of a workshop sponsored by the William B. Ruger Chair of National Security Economics, Newport, R.I.: Naval War College, May 19–21, 2010, pp. 259–272.

2. لعل القراء الأذكياء يرون عبارة "الخوف، والغموض، والشك"، وهي عبارة صاغها جين أمدال Gene Amdahl بعد تركه شركة آي بي أم للكمبيوتر IBM، ليصف الأثر الذي قام الناس «بغرسه في أذهان المتعاملين المحتملين الذين يمكن أن يفكروا بمنتجات أمدال».

3. انظر:

John J. Mearsheimer, *Conventional Deterrence*, Ithaca, N.Y.: Cornell University Press, 1985.

4. على الرغم من أن الآثار النفسية للهجوم عبر الإنترنت تُعتبر تخمينية، فإنها يمكن أن تتجاوز آثارها الحقيقية. على سبيل المثال، إذا قام المرء فقط بتعداد عدد أجهزة الطرد المركزي التي دمرت نفسها، فإن ستكسنت لم يسبب سوى تأخير في البرنامج النووي الإيراني لبضعة أشهر. ولكن لكي تحصل إيران على قنبلة، لابد لها أن تلتزم بتخصيب اليورانيوم من 3٪ (U-235) حتى 90٪. وأثناء الشهور اللازمة للقيام بذلك، قد ترد الجيوش الغربية على الأغلب بالإنذار والقوة. فإذا لم تفلح إيران في إقناع نفسها بأن ستكسنت لم يتم اجتثاثه، فقد تخشى بشكل ملحوظ أن يتم توجيه أمر لأجهزة الطرد المركزي بالتعطل في تلك الشهور الحرجة، الأمر الذي يعرّض إيران للانتقام دون أن تحصل على قنبلة بعد كل هذا الجهد، وبذلك يسبب توقفاً قبل أن تفكر بالمضي قدماً.

5. عندما يتم تشفير رمز هجوم ما، فإن عملية فك التشفير تكون بطيئة جداً حتى إذا كانت ممكنة. وقد تم تشفير جزء من ستكسنت ولكن تم فكُّه في ما بعد. في منتصف آب/ أغسطس 2012 لم تستطع كاسبرسكي Kaspersky، وهي شركة أمنية كبرى، فك التشفير في برمجيات التجسس "غوس" Gauss، وأصدرت نداء عاماً طلباً للمساعدة.

(Jeff Goldman, "Kaspersky Seeks Help Decrypting Gauss Malware Payload," *eSecurity Planet*, August 15, 2012).

6. ماكيروفا *Makirovka* هو مصطلح روسي يعني: «التمويه، والخداع، والإخفاء».

7. انظر:

M. Taylor Fravel and Evan S. Medeiros, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security*, Vol. 35, No. 2, Fall 2010, pp. 48–87; and Roger Cliff, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States*, Santa Monica, Calif.: R AND Corporation, MG-524-AF, 2007.

8. إيران ماضية في فصل شبكتها الخاصة بالإنترنت عن بقية العالم. فقد ورد في:

Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet," *Wall Street Journal*, May 28, 2011:

يوم الجمعة ظهرت تقارير جديدة في الصحافة المحلية تفيد بأن إيران كانت تنوي أيضاً تجديد نظام تشغيل حواسيبها في الشهور القادمة لكي تبدّل نظام ويندوز من شركة مايكروسوفت. وقد تم نسبة هذا التطور - الذي لم يكن بالإمكان تأكيده من مصادر مستقلة - إلى وزير الاتصالات الإيراني رضا تاغيبور.

انظر أيضاً: "Iran to Unveil National OS Soon," *PressTV*, January 4, 2011.

9. تتمثل إحدى طرق البرهنة على قدرات الهجوم عبر الإنترنت في مهاجمة دولة تستحق أن تُهاجم بوضوح، وبحيث يصبح مصيرها درساً للآخرين. ويُفترض بهذه الدولة أن تكون ممن يعتمدون على بعض البنى التحتية، لكنها ضعيفة في حمايتها. وتفيد هذه الطريقة إذا لم تكن الدولة المستهدفة بصورة عامة ودية، وليس هناك خيار جيد لاستجابتها دون تصعيد الأمور لدرجة أكبر مما هي مستعدة للتعامل معه. لكن، إجمالاً، يوجد مبررات أكثر من كافية للنصح بعدم تجربة ذلك. ويتطلب التأثير نوعاً من الإيعاز إلى الدولة المهاجمة بوصفها الفاعل، وإن بشكل مفهوم ضمناً على الأقل، وإلا فإن الشيء الوحيد الذي يتم استعراضه والبرهنة عليه هو أن بعض الدول تبني بنى تحتية لا تستطيع الدفاع عنها. ولكن مثل هذه السياسة تجعل المهاجم يبدو متنمراً، كما تُضفي الشرعية على الحرب عبر الإنترنت. وقد تُعجب دولٌ أخرى بجرأة المهاجم، ولكن ليس بالضرورة بفطنته. ومن السهل جداً

على الذين يثيرون الإعجاب أن يواجهوا حقيقة أنهم نادراً ما يكونون ضعفاء وعرضة للهجوم مثل الدولة التي تمت مهاجمتها. فإذا أتيح الهجوم من خلال نقطة الضعف التي يشترك الآخرون فيها، فمن الممكن أن يأخذوا نتائج الهجوم على محمل الجد، ولكن لفترة تكفي لإصلاح نقاط الضعف بأنفسهم.

10. إذا كانت الدولة المستهدفة ترى أن احتمال أن تنفذ الدولة "ع" هجوماً ثانياً عبر الإنترنت – وربما أكثر أهمية – رداً على شيء قد تفعله هي، بما نسبته 50:50 (أي مساوية بالضبط لاحتمال أن تعتقد أن الدولة "ع" قد نفذت الهجوم عبر الإنترنت)، فسوف تقوم بوزن التكلفة المتوقعة عليها من رد فعل الدولة "ع"، إذا قررت المضي والتنفيذ بنصف الشدة التي كانت ستنفذها لو تأكد لها أن الدولة "ع" هي التي نفذت الهجوم عبر الإنترنت.

11. للتوضيح بالقدر نفسه، افترض أن الدولة المستهدفة تعتقد أن احتمال أن تكون الدولة المهاجمة هي "ص" مثل احتمال أن تكون "ع" (ولكنها لا تعتقد أن "ص" و"ع" تواطأتا). فإذا انتقمت من واحدة، فلِمَ لا تنتقم من الأخرى؟ والسبيل الوحيدة التي يمكن تبريرها هي إذا اعتقدت الدولة المستهدفة أن عواقب ضرب دولة بريئة "ص"، أسوأ من عواقب ترك الدولة "ع" تنجو من آثار الهجوم.

12. الولايات المتحدة تردُّ بعنف عندما تعتقد أنها قد هوجمت، حتى إذا دلت الحقائق على خلاف ذلك. وقد اكتشف الإسبان هذا بعد غرق البارجة الأمريكية "ماين" USS Maine عام 1898، من خلال ما يُعتقد الآن أنه حادث وليس لغماً. وإذا أخذنا هذا في الاعتبار، فإن الرد العنيف ليس ضمانة، كما دل على ذلك عدم الرد على الاستيلاء عام 1968 على البارجة الأمريكية "بويبلو" USS Pueblo، والهجوم الصاروخي العراقي على البارجة الأمريكية "ستارك" USS Stark.

13. بين الذين قدَّموا حججاً مماثلة:

Robert Pape (in Robert A. Pape, *Bombing to Win: Air Power and Coercion in War*, Ithaca, N.Y.: Cornell University Press, 1996); David Johnson (in David E. Johnson, Karl P. Mueller, and William H. Taft, *Conventional Coercion Across the Spectrum of Operations: The Utility of U.S. Military Forces in the Emerging Security Environment*, Santa Monica, Calif.: R AND Corporation, MR-1494-A, 2003); Karl Mueller (in Karl P. Mueller, Jasen J. Castillo, Forrest E. Morgan, Negeen Pegahi, and Brian Rosen, *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*, Santa Monica, Calif.: R AND Corporation, MG-403-AF, 2006), Daniel Byman (in Daniel Byman, Matthew Waxman, and Eric V. Larson, *Air Power as a Coercive Instrument*, Santa Monica, Calif.: R AND Corporation, MR-1061-AF, 1999); and Forrest Morgan (in Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica, Calif.: R AND Corporation, MG-614-AF, 2008).

14. انظر على سبيل المثال:

Thomas C. Schelling, *Arms and Influence*, New Haven, Conn.: Yale University Press, 1966, notably Chapter Three.

15. خير مثال على هذه الحجة هو:

David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, p. 1.

في مقابلة سابقة سألت مليسا لي Melissa Lee وزير الدفاع في ذلك الوقت وليام لين William Lynn عن هذا. وفقاً لأحد التقارير (Kim Zetter, "Senior Defense Official Caught Hedging on U.S. Involvement in Stuxnet," *WIRED*, May 26, 2011) فقد سألت لي لين مباشرة: «هل الولايات المتحدة متورطة بأي شكل من الأشكال في تطوير ستكسنت؟» فكان رد لين طويلاً بحيث لا يلاحظ مشاهد المقابلة أنه لم يجب عن السؤال؛ إذ أجاب لين: «تحديات ستكسنت، كما قلت، تريكم صعوبة أي عملية إسناد إلى فاعل ما، وهي شيء ما نزال ننظر فيه، ومن الصعب الدخول في أي نوع من المداخلات على ذلك إلى أن ننتهي من فحوصاتنا». قالت لي: «سيدي، أنا لا أسألك إن كنت تعتقد أن دولة أخرى متورطة». وتصر لي قائلة: «إنني أسألك إن كان ثمة دولة أخرى متورطة». وأخيراً قال لين: «هذا ليس أمراً سنكون قادرين على الإجابة عنه عند هذه النقطة».

16. انظر:

Ellen Nakashima, "With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace," *Washington Post*, May 30, 2012, p. A1.

لكن ورد في إعلان وكالة مشروعات الأبحاث الدفاعية المتقدمة: «إن برنامج الخطة "س" صراحة لا يقوم بتمويل... جيل أسلحة الفضاء الإلكتروني».

(DARPA, "Cyber Experts Engage on DARPA's Plan X," press release, October 17, 2012).

17. ورد في:

"Cyber Strikes a 'Civilized' Option: Britain," *Technology Inquirer*, Agence France-Presse, June 3, 2012.

وورد في هذا المصدر ما نصه: «إن الضربات الاستباقية عبر الإنترنت ضد تهديدات الأمن القومي المتصورة هي "خيار حضاري" لتحييد الهجمات المحتملة، وذلك حسبما صرّح به نيك هارفي وزير الدولة لشؤون القوات المسلحة البريطانية. وأدلى هارفي بهذا التصريح في القمة الأمنية "حوار شانجريلا" التي انعقدت في سنغافورة، تعليقاً على تقارير تفيد بأن الولايات المتحدة قد أطلقت هجمات عبر الإنترنت بهدف شل البرنامج النووي الإيراني. وأيّد الوزيرُ البريطاني وزيرَ الدفاع الكندي بيتر جوردون ماكاي Peter Gordon MacKay، الذي شبَّه الضربة الاستباقية عبر الإنترنت بـ "بوليصة التأمين"».

18. انظر:

Department of Defense, Office of General Counsel, *An Assessment of Legal Issues in Information Operations*, May 1999.

الفصل الثالث

1. إذا تم منح الولايات المتحدة الخيار بين امتلاك قدرة ردع نووية والقدرة على التلويح بقدرات الهجوم عبر الإنترنت، فمن الواضح أن الخيار الأول سيكون هو المفضل. والردع النووي موجود بالفعل، ومع هذا فإن الأوساط الاستراتيجية الأمريكية تشعر بالقلق حيال امتلاك الدول المارقة أسلحة نووية. وتذهب السياسة الأمريكية بعيداً لكي تمنع إيران من حيازة أسلحة نووية. ويدل هذا على أنه ليس هناك ثقة كاملة بأن بإمكان الولايات المتحدة دائماً ردع استخدام الأسلحة النووية في الظروف كافة. إنه السياق الذي نسأل أنفسنا فيه: هل من الممكن أن يكون التلويح بالقدرات الهجومية عبر الإنترنت فيه بعض المساعدة هنا؟

2. إن التركيز على "الفوز" في مواجهة نووية ليس الحجة التي تقول بأن على الولايات المتحدة استخدام هذه التكتيكات بوصفها الأسلوب الوحيد أو الرئيسي لنزع فتيل تهديد دول نووية مارقة. ويمكن قول الكثير عن سياسات ما قبل الأزمة لإزالة الحافز أو القدرة لدى الدول المارقة على امتلاك أسلحة نووية، وعن سياسات في أثناء الأزمة تسعى لإقناع الدولة المارقة بأن عليها اتباع معايير السلوك الدولية، وعن السياسات التي تمنح الدولة المارقة مخرجاً مشرفاً حتى من مأزق صنعته هي لنفسها.

3. من أجل معرفة المنشأ، سوف يتجاهل هذا التحليل العديد من الخيارات والنقاط الفرعية التي توجد حتى في أبسط مواجهة نووية من هذا النوع. على سبيل المثال، إذا كان التهديد من الدولة النووية المارقة مفهوماً ضمناً، فقد لا يكون من الواضح أن أي إجراء أمريكي يتجاوز الخط. في مثل هذه الظروف، ومن خلال عدم الاستجابة، يقل مستوى إراقة ماء الوجه بالنسبة إلى الدولة المارقة. لكن إذا استنتجت الولايات المتحدة أن التهديدات المبطنة تبدو جوفاء في إحدى المرات، فقد تشعر بأنها بمأمن من المشكلات. أما إذا أرادت الدولة المارقة الاحتفاظ بقدرتها على التهديد، فقد يكون عليها أن تجد عتبة ثانية (أو ما هو أصعب من ذلك، تحاول أن تجبر الولايات المتحدة على الانسحاب أو تتجنب التكرار) وتنتقل إلى تهديد واضح. كذلك قد تكون ثمة عتبات متعددة للاستخدام النووي، بعضها قد يدعو إلى انتقام شامل وبعضها الآخر لا يفعل ذلك. قد تشمل الخيارات من حيث الشدة: ضربة استعراضية، وانفجاراً يدمِّر المعدات دون الناس (مثل، النبض الكهروطيسي)، وهجوماً ضد السفن وضد الأسطول، وهجوماً على القوات البرية، وهجوماً على مركز سكاني حليف، وهجوماً على الأراضي الأمريكية.

4. لكن ماذا لو أن تصميم أحد الطرفين، لكي يجعل الطرف الآخر يتصرف بطريقة مقبولة، هيمن على قاعدة تحسين نتائجه؟ ينبغي عدم استبعاد مثل هذه الإمكانية وأن تؤخذ على محمل الجد؛ فالناس يعاقبون المخادعين بشدة، حتى على حساب رفاهيتهم في حالات تشبه الألعاب. وقد أظهر الاقتصاديون مراراً ما يشبه ذلك، ولاسيما بمراقبة الناس يلعبون "لعبة الإنذار الأخير"، حيث يتفاعل لاعبان ليقرِّرا كيف يقسمان مبلغاً من المال أعطي لهما.

(Martin A. Nowak, Karen M. Page, and Karl Sigmund, "Fairness Versus Reason in the Ultimatum Game," *Science*, Vol. 289, No. 5485, September 2000, pp. 1773–1775).

وفي الواقع، يمكن ربط هذه الميول. انظر مثلاً:

Marco F. H. Schmidt and Jessica A. Sommerville, "Fairness Expectations and Altruistic Sharing in 15-Month-Old Human Infants," *PLOS ONE*, Vol. 6, No. 10, October 7, 2011).

5. تُستخدم هنا "دورة القيادة والتحكم النووية" بشكل متساهل لتدل، ليس على الصلة بين الأمر بإطلاق سلاح نووي و/ أو تفجير قنبلة نووية فحسب، وإنما أيضاً على سلامة التعليمات في الأسلحة ذات الصلة نفسها. والإخفاق في هذه الأخيرة، مثلاً، يمكن أن يؤدي إلى الخطأ في الإطلاق، أوضعف الهدف، أو فشل الانفجار، أو التفجير قبل أوانه.

6. قام زميل في راند بالتخمين: لماذا تكلف الولايات المتحدة نفسها عناء التلويح بأن بإمكانها تعطيل تشغيل نظام القيادة والسيطرة النووي للدولة المارقة، بدلاً من تعطيله بالفعل؟ ذلك هو المنع وليس التلويح. إذا كانت الإجابة أن الولايات المتحدة قد لا تكون قادرة على منع عملية الإطلاق، ولكنها تريد أن تجعل الدولة المارقة تصدّق أنها قادرة على فعل ذلك، فلا بد من قيام الولايات المتحدة بالاحتيال والخداع. وبما أن المنع هو الأفضل بشكل واضح - بالنظر إلى المخاطر النووية - من مجرد استعراض القدرة على المنع، فإن ذلك يستتبع أن ينطوي التلويح ضمناً على الخداع.

مع أخذ هذا المنطق في الاعتبار، تفترض الدولة المارقة أن أي هجوم أمريكي عبر الإنترنت لم يمنع في الواقع إطلاق الأسلحة النووية هو بمنزلة خداع. وثمة رد أولي على ذلك النوع من المنطق، هو أن الولايات المتحدة - بتلويحها بالقدرة على وقف الدورة النووية للدولة المارقة - تعلن أنها قد منعت بالفعل عملية الإطلاق، وأنها أرادت فقط أن تعرف الدولة المارقة ذلك بحيث إنها لا تضع نفسها نتيجة لذلك في موقف لا تستطيع فيه التراجع، بل قد تضطر إلى التقهقر، مع أنها حتى ذلك الوقت لاتزال واثقة من أنها تملك القدرة على تنفيذ ضربة نووية. بعد ذلك، قد تفكر الدولة المارقة في أن التلويح الأمريكي بهذه القدرة يمكن ألا يسفر إلا عن تكلفة تتكبدها الولايات المتحدة؛ لأنه سيزيد من احتمالات اكتشاف نقطة الضعف التي سمحت بشن الهجوم عبر الإنترنت. ولكي تأخذ الدولة المارقة التلويح على محمل الجد (وليس على سبيل الخدعة)، سيكون عليها أن تعتبر أن الولايات

المتحدة تعتقد أن إمكانية نزع فتيل الأزمة قبل أن تضع الدولة المارقة نفسها في موقف محفوف بالمخاطر لكلا الطرفين، تفوق إمكانية أن يؤدي اكتشاف نقطة الضعف إلى تعريض الهجوم عبر الإنترنت للخطر.

7. صحيح أن الهجوم عبر الإنترنت الذي يمكن أن يعطل شيئاً سيكون له تأثير أطول، ولكن من الأسهل كثيراً التدخل في تسلسل قيادة معقد، من إدخال أمر مدمر في تسلسل قيادة معقد ذي مزايا آمنة تحميه من الإخفاق والفشل. وإن كون ستكسنت قد دمر أجهزة الطرد المركزي الإيرانية دون إحداث نقص خطير في إنتاج إيران لليورانيوم، يدل على أن هذه الأجهزة كانت في مرحلة بدء التشغيل. تتم إعادة برمجة الأجهزة في هذه المرحلة بصورة متكررة، ولهذا، فهي أكثر عرضة للأخطاء التي تسببها البرمجة من الأجهزة التي تعمل بشكل مستمر منذ فترة طويلة.

8. يتفق هذا تماماً مع نموذج التدخل الافتراضي. افرض أن الدولة المارقة تعتقد أن عدد نقاط الخلل التي يمكن استغلالها في نظامها هو قيمة متغيرة مع توزيع بديهي للاحتمالية، وذلك كما يلي: نسبة احتمال 80٪ بعدم وجود نقاط خلل، و10٪ بوجود خلل واحد، و10٪ بوجود خللين. العدد المتوقع لنقاط الخلل هو 0.3 (80٪ × 0 + 10٪ × 1 + 10٪ × 2). بعد ذلك يتم اكتشاف نقطة خلل وإزالتها. وهذا يلغي إمكانية أن النظام لم تكن تشوبه شائبة. ومع ذلك، فإنه لا يتطرق إلى ما إذا كان النظام بدأ بنقطة خلل واحدة أو اثنتين، وما إذا كانت كلتاهما بالمستوى نفسه من الاحتمال من قبل، وكذلك في ما بعد (إذا كان ثمة أيٌّ من نقاط الخلل، فإن اكتشاف واحدة يعزز دلائل وجود اثنتين). لذا، فإنه بمجرد إزالة خلل يكون هنالك الآن احتمال بنسبة 50٪ بأنه لا تبقى أي نقاط خلل، و50٪ باحتمال وجود نقطة خلل واحدة متبقية. ويُعتبر عدد نقاط الخلل بعد الاكتشاف والإزالة 0.5 (50٪ مضروباً بصفر مضافاً إليه 50٪ مضروباً بـ 1). وهكذا نجد أنه في أثناء اكتشاف نقطة خلل وإصلاحها - في الوقت الذي انخفض فيه العدد الفعلي لنقاط الخلل بمقدار واحدة - ارتفع العدد المتوقع لبقية نقاط الخلل في الواقع بمعدل 0.2.

9. يمكن أن يكون ثمة استثناء وهو اتحاد "العيون الخمس" Five Eyes consortium؛ المكون من الولايات المتحدة الأمريكية والمملكة المتحدة ونيوزيلندا وأستراليا وكندا، والتي تتشارك معها معلومات مفصلة بصورة مستمرة.

10. تنشط مقايضات مألوفة لتقدير إذا ما كان ينبغي إخفاء مثل هذه الملاحظات عن الدولة المارقة. فإذا اكتشفت الدولة المارقة أن شيئاً غير متوقع يحدث في دورة قيادتها وسيطرتها النووية، فقد يدفعها ذلك إلى الاهتمام بنقاط الخلل الممكنة لديها، ولكن أيضاً قد يجري تحذيرها من الوقوع في وضع مربك. لكن الكشف عن ماهية الضربة التي سببت التأثير غير مفيد؛ لأن ذلك سيجعل إصلاح نقاط الخلل أسهل من دون المساهمة كثيراً في المصداقية المضادة لتهديد الحرب عبر الإنترنت.

المراجع

Alexander, Keith, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," statement to the U.S. Senate Committee on Armed Services, April 15, 2010, p. 21. As of June 29, 2011:http://www.armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf

Byman, Daniel L., Matthew C. Waxman, and Eric Larson, *Air Power as a Coercive Instrument*, Santa Monica, Calif.: RAND Corporation, MR-1061-AF, 1999. As of January 29, 2013:http://www.rand.org/pubs/monograph_reports/MR1061.html

Cliff, Roger, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States*, Santa Monica, Calif.: RAND Corporation, MG-524-AF, 2007. As of January 28, 2013:http://www.rand.org/pubs/monographs/MG524.html

"Cyber Strikes a 'Civilized' Option: Britain," *Technology Inquirer*, Agence France-Presse, June 3, 2012. As of June 3, 2012: http://technology.inquirer.net/11747/cyber-strikes-a-civilized-option-britain

Defense Advanced Research Projects Agency, "Cyber Experts Engage on DARPA's Plan X," press release, October 17, 2012. As of February 19, 2013:http://www. darpa.mil/NewsEvents/Releases/2012/10/17.aspx

Department of Defense, Office of General Counsel, "An Assessment of Legal Issues in Information Operations," May 1999.

Fravel, M. Taylor, and Evan S. Medeiros, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security*, Vol. 35, No. 2, Fall 2010, pp. 48–87.

Goldman, Jeff, "Kaspersky Seeks Help Decrypting Gauss Malware Payload," *eSecurity Planet*, August 15, 2012. As of August 25, 2012:http://www.esecurityplanet. com/malware/kaspersky-seeks-help-decrypting-gauss-malware-payload.html

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 1, November 11, 2010.

"Iran to Unveil National OS Soon," *PressTV*, January 4, 2011. As of June 3, 2012:http://www.presstv.ir/detail/158534.html

Johnson, David E., Karl P. Mueller, and William H. Taft, *Conventional Coercion Across the Spectrum of Operations: The Utility of U.S. Military Forces in the Emerging Security Environment*, Santa Monica, Calif.: RAND Corporation, MR-1494-A, 2003. As of January 28, 2013:http://www.rand.org/pubs/monograph_reports/MR1494.html

Libicki, Martin C., *Cyberdeterrence and Cyberwar*, Santa Monica, Calif.: RAND Corporation, MG-877-AF, 2009. As of January 28, 2013:http://www.rand.org/pubs/monographs/MG877.html

———, "Wringing Deterrence from Cyberwar Capabilities," in Richmond M. Lloyd, ed., *Economics and Security: Resourcing National Priorities*, proceedings of a workshop sponsored by the William B. Ruger Chair of National Security Economics, Newport, R.I.: Naval War College, May 19–21, 2010, pp. 259–272.

Masters, Jonathan, "Confronting the Cyber Threat," New York: Council on Foreign Relations, May 23, 2011. As of February 4, 2013: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

Mearsheimer, John J., *Conventional Deterrence*, Ithaca, N.Y.: Cornell University Press, 1985.

Morgan, Forrest E., Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica, Calif.: RAND Corporation, MG-614-AF, 2008. As of January 28, 2013: http://www.rand.org/pubs/monographs/MG614.html

Mueller, Karl P., Jasen J. Castillo, Forrest E. Morgan, Negeen Pegahi, and Brian Rosen, *Striking First:*

Preemptive and Preventive Attack in U.S. National Security Policy, Santa Monica, Calif.: RAND Corporation, MG-403-AF, 2006. As of January 28, 2013:

http://www.rand.org/pubs/monographs/MG403.html

Nakashima, Ellen, "With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace," *Washington Post*, May 30, 2012, p. A1.

Nowak, Martin. A., Karen M. Page, and Karl Sigmund, "Fairness Versus Reason in the Ultimatum Game," *Science*, Vol. 289, No. 5485, September 2000, pp. 1773–1775.

Pape, Robert A., *Bombing to Win: Air Power and Coercion in War*, Ithaca, N.Y.: Cornell University Press, 1996.

Quester, George H., *Deterrence Before Hiroshima*, Piscataway, N.J.: Transaction Publishers, 1986.

Rhoads, Christopher, and Farnaz Fassihi, "Iran Vows to Unplug Internet," *Wall Street Journal*, May 28, 2011. As of June 3, 2012: http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html

Sanger, David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, p. 1.

Schelling, Thomas C., *Arms and Influence*, New Haven, Conn.: Yale University Press, 1966.

Schmidt, Marco F. H., and Jessica A. Sommerville, "Fairness Expectations and Altruistic Sharing in 15-Month-Old Human Infants," *PLOS ONE*, Vol. 6, No. 10, October 7, 2011.

تصوير أحمد ياسين

Sterner, Eric, "Stuxnet and the Pentagon's Cyber Strategy," Arlington, Va.: George C. Marshall Institute, October 13, 2010. As of January 2013:

http://www.marshall.org/article.php?id=918

Zetter, Kim, "Senior Defense Official Caught Hedging on U.S. Involvement in Stuxnet," *WIRED*, May 26, 2011. As of May 27, 2012:

http://www.wired.com/threatlevel/2011/05/defense-department-stuxnet/

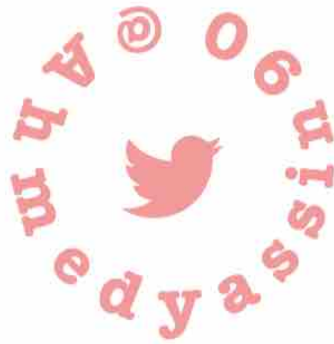
تصوير
أحمد ياسين

نبذة عن المؤلف

مـارتن سي. ليبيكـي **Martin C. Libicki**؛ خبـير أول في مجـال الإدارة بمؤسـسة رانـد، وتتركز أبحاثه حول تأثيرات تكنولوجيا المعلومـات في الأمـن الـداخلي والـوطني. وهـو حاصل على درجة الدكتوراه في الاقتصاد الصناعي من جامعة كاليفورنيا ببيركلي.

تصوير

أحمد ياسين



تصوير
أحمد ياسين
تويتر
@Ahmedyassin90



Panton 340 C

التلويح بقدرات الهجوم عبر الأنترنت

مارتن سي. ليبيكي

تصوير

أحمد ياسين



مركز الإمارات للدراسات والبحوث الاستراتيجية

العدد 124